Vysoká škola báňská – Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra telekomunikační techniky

Bezpečnostní rizika v optických přístupových sítích

Security Risks in Optical Access Networks

2014 Vojtěch Resutík

VŠB - Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra telekomunikační techniky

Zadání bakalářské práce

Student: **Vojtěch Resutík**

Studijní program: B2647 Informační a komunikační technologie

Studijní obor: 2601R013 Telekomunikační technika

Téma: Bezpečnostní rizika v optických přístupových sítích
Security Risks in Optical Access Networks

Zásady pro vypracování:

Díky postupnému rozvoji a nasazování pasivních optických přístupových sítí v praxi dojde k pokrytí širokého počtu domácností a koncových uživatelů výkonným přístupovým řešením, což mimo jiné umožní vznik a přístup k řadě moderních multimediálních a interaktivních služeb. V souvislosti s tím se však objevuje nutnost dostatečného zabezpečení přenášených dat i vlastní optické sítě proti různým druhům bezpečnostních rizik. Cílem absolventské práce je popsat nejvážnější bezpečností hrozby v současné generaci pasivních optických sítí.

1. Popište bezpečnostní hrozby v současné generaci pasivních optických sítích typu EPON (GEPON, 10GEPON), GPON (XG-PON) a nutnosti jejich zabezpečení.
2. Popište bezpečnostní hrozby při nasazení optických přístupových sítí WDM-PON a sítí nové generace obecně.
3. V laboratorních podmínkách proveďte experimentální měření bezpečnostních rizik optické přístupové sítě WDM-PON včetně bezpečnostních rizik souvisejících s nasazením WDM-PON na stávající optické přístupové sítě (přístupové sítě typu WDM-TDM).

Seznam doporučené odborné literatury:

PRAT, Josep. *Next-Generation FTTH Passive Optical Networks: Research towards unlimited bandwidth access*. Barcelona: Springer, 2008. 187 p. ISBN 978-1-4020-8469-0.

LAM, Cedric. *Passive Optical Networks: Principes and practice*. Oxford: Elsevier Inc., 2007. 324 p. ISBN 978-0-12-373853-0.

Formální náležitosti a rozsah bakalářské práce stanoví pokyny pro vypracování zveřejněné na webových stránkách fakulty.

Vedoucí bakalářské práce: **Ing. Petr Koudelka**

Datum zadání: 01.09.2013

Datum odevzdání: 07.05.2014

doc. Ing. Miroslav Vozňák, Ph.D.
vedoucí katedry

prof. RNDr. Václav Snášel, CSc.
děkan fakulty

Prohlášení studenta

Prohlašuji, že jsem tuto bakalářskou práci vypracoval samostatně. Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.

V Ostravě ....7.5. 2014..... .....Vojtěch Rezník.....

Poděkování

Na tomto místě bych rád poděkoval svému vedoucímu bakalářské práce Ing. Petru Koudelkovi za odbornou pomoc, ochotu a vstřícný přístup při vytváření této práce. Dále bych rád poděkoval své rodině za projevenou podporu a poskytnutí zázemí a podmínek k dokončení studia.

Abstrakt

Tato bakalářská práce se zabývá problematikou bezpečnosti optických přístupových sítí, konkrétně pasivní varianty optických sítí (PON). V první části práce jsou popsány vlastnosti technologií současné i budoucí generace sítí PON, včetně možností jejich zabezpečení. V druhé části jsou popsány bezpečnostní rizika systémů založených na metodě časového dělení TDM-PON, vlnového dělení WDM-PON a bezpečnostní mechanismy používané k jejich zamezení. V praktické části jsou v laboratorních podmínkách ověřena bezpečnostní rizika spojená s nasazením technologie WDM-PON.

Klíčová slova: bezpečnost, bezpečnostní rizika, optická přístupová síť, PON, TDM-PON, WDM-PON

Abstract

This bachelor thesis deals with security of optical access networks, specifically its passive optical networks variants (PON). The first part describes the characteristics of technologies, both current and future generations of the PON networks, including possibilities of their securing. The second part describes the security risks of systems based on the method of time division multiplexing TDM-PON, wavelength division multiplexing WDM-PON and security mechanisms used to avoid them. The aim of the work in the practical part is to verify in laboratory conditions security risks associated with the deployment of the WDM-PON technologies.

Keywords: security, security risks, optical access network, PON, TDM-PON, WDM-PON

Seznam použitých zkratek a symbolů

10GEPON	–	10 Gbit/s Ethernet Passive Optical Network
3DES	–	Triple Data Encryption Standard
ADSL	–	Asymmetric Digital Subscriber Line
AES	–	Advanced Encryption Standard
AON	–	Active Optical Network
APON	–	ATM Passive Optical Network
ATM	–	Asynchronous Transfer Mode
AWG	–	Arrayed Waveguide Grating
BPON	–	Broadband Passive Optical Network
CMAC	–	Cipher based Message Authentication Code
CPON	–	Composite Passive Optical Network
CRC	–	Cyclic Redundancy Check
CWDM	–	Coarse Wavelength Division Multiplexing
DBA	–	Dynamic Bandwidth Allocation
DBRu	–	Dynamic Bandwidth Report upstream
DES	–	Data Encryption Standard
DoS	–	Denial of Service
DH	–	Diffie-Hellman
DoS	–	Denial Of Service
DWA	–	Dynamic Wavelength Allocation
DWDM	–	Dense Wavelength Division Multiplexing
ECC	–	Elliptic Curve Cryptography
EDFA	–	Erbium Doped Fibre Amplifier
EPON	–	Ethernet Passive Optical Network
FCS	–	Frame Check Sequence
FDM	–	Frequency Division Multiplexing
FEC	–	Forward Error Correction
FSAN	–	Full Service Access Network
FTTB	–	Fibre To The Building
FTTC	–	Fibre To The Curb
FTTH	–	Fibre To The Home
FTTN	–	Fibre To The Node

FTTO – Fibre To The Office
FTTP – Fibre To The Premises
FTTx – Fibre To The x
FTTx – Fibre To The x
GEM – GPON Encapsulation Method
GPON – Gigabit-capable Passive Optical Network
GTC – GPON Transmission Convergence Layer
HDSL – High-bit-rate Digital Subscriber Line
HEC – Header Error Detection and Correction
ID – Identificator
IEEE – Institute of Electrical and Electronics Engineers
ISDN – Integrated Services Digital Network
ITU-T – International Telecommunication Union-Telecommunication Standardization Sector
KEK – Key Encryption Key
LAN – Local Area Network
LLID – Logical Link Identificator
MAC – Media Access Control
MPCP – Multipoint Control Protocol
MSK – Master Session Key
NG-PON – Next Generation Passive Optical Network
OAN – Optical Access Network
ODN – Optical Distribution Network
OLT – Optical Line Termination
OMCI – ONU Managment and Control Interface
ONT – Optical Network Terminal
ONU – Optical Network Unit
PCBd – Physical Control Block downstream
PLOAM – Physical Layer Operations And Maintenance
PLOAMu – PLOAM upstream field
PLI – Payload Length Indicator
PLOu – PLOAM upstream field
PLSu – Power Levelling Sequence upstream

Port-ID	–	Port Identificator
PON	–	Passive Optical Network
PSBd	–	Physical Synchronization Block downstream
PTI	–	Payload Type Indicator
P2P	–	Point to Point
P2MP	–	Point to Multipoint
QoS	–	Quality of Service
RADIUS	–	Remote Authentication Dial In User Service
RS	–	Reed-Solomon
RSA	–	Rivest, Shamir, Adleman
SK	–	Session Key
TDM	–	Time Division Multiplexing
TDMA	–	Time Division Multiple Access
TDM-PON	–	Time Division Multiplexing Passive Optical Network
VDSL	–	Very-high-bit-rate Digital Subscriber Line
WDM	–	Wavelength Division Multiplexing
WDM-PON	–	Wavelength Division Multiplexing Passive Optical Network
XG-PON	–	XG Passive Optical Network
XGEM	–	XG-PON Encapsulation Method
XGTC	–	XG-PON Transmission Convergence Layer
λ	–	Lambda, značení vlnové délky

Obsah

Úvod **6**

1 Optické přístupové sítě **7**
1.1 Dělení optických přístupových sítí 7
1.2 Funkční celky optické přístupové sítě 8
1.3 Uspořádání FTTx 9

2 Technologie TDM-PON **11**
2.1 Topologie PON 13
2.2 APON/BPON (ITU-T G.983) 14
2.2.1 Zabezpečení APON 15
2.3 GPON (ITU-T G.984) 15
2.3.1 Přenos v GPON 16
2.3.2 Zabezpečení GPON 19
2.4 XG-PON (ITU-T G.987) 20
2.4.1 Přenos v XG-PON 22
2.4.2 Zabezpečení XG-PON 24
2.4.3 Derivace bezpečnostních klíčů 26
2.5 EPON (IEEE 802.3ah) 27
2.5.1 Přenos v EPON 28
2.5.2 Zabezpečení EPON 29
2.6 10GEPON (IEEE 802.3av) 30
2.6.1 Zabezpečení 10GEPON 31
2.7 Porovnání technologií TDM-PON 31

3 Technologie WDM-PON **32**
3.1 CWDM 32
3.2 DWDM 33
3.3 Varianty WDM-PON 33
3.4 Princip AWG 37

4 Bezpečnost sítě **38**
4.1 Bezpečnostní rizika systémů TDM-PON 38
4.1.1 Odposlech služebních zpráv 38
4.1.2 Odposlech ve vzestupném směru 39
4.1.3 Odposlech v sestupném směru 39

4.1.4 Impersonace . . . 40
4.1.5 Odepření služby . . . 40
4.2 Bezpečnostní rizika systémů WDM-PON . . . 40
4.3 Šifrování . . . 41
4.3.1 Šifra Churning . . . 41
4.3.2 Symetrické šifrování . . . 42
4.3.3 Asymetrické šifrování . . . 45
4.4 Kódování FEC . . . 46
4.4.1 Reed-Solomon . . . 46
4.5 Autentizace . . . 47
4.5.1 Autentizace podle hesla . . . 47
4.5.2 Autentizace podle registračního ID . . . 47
4.5.3 Autentizace IEEE 802.1X . . . 48

5 Praktické měření **50**
5.1 Popis měřícího pracoviště a použité přístroje . . . 50
5.2 Konfigurace zařízení . . . 52
5.3 Spektrální analýza navržených topologií . . . 55
5.4 Simulace v programovém prostředí Optiwave . . . 58

Závěr **65**

Literatura **66**

Přílohy **70**

Seznam tabulek

2.1 Varianty rychlostí technologie APON/BPON. 14
2.2 Varianty rychlostí technologie GPON. 16
2.3 Porovnání technologií TDM-PON. 31
5.1 Parametry spektra na kanálu č.2 před a po aktivaci jednotky na kanálu č. 1. 56
5.2 Parametry spektra na jednotce ONU připojené na kanálu č. 7 před a po aktivaci jednotek na kanálech č. 6 a 8. 58
5.3 Parametry signálů spektra na výstupu sdružovače. 61
A.1 Parametry spektra na kanálu č. 7 před a po aktivaci jednotky na kanálu č. 6. A-I
A.2 Parametry spektra na kanálu č.9 před a po aktivaci jednotky na kanálu č. 8. A-II
A.3 Parametry spektra na kanálu č. 9 před a po aktivaci jednotky na kanálu č. 10.A-III
A.4 Parametry spektra na kanálu č. 20 před a po aktivaci jednotky na kanálu č. 21. . . . . A-IV
A.5 Parametry spektra na kanálu č. 28 před a po aktivaci jednotky na kanálu č. 27. . . . . A-V
A.6 Parametry spektra na kanálu č. 31 před a po aktivaci jednotky na kanálu č. 32. . . . . A-VI

Seznam obrázků

1.1 Rozdělení optických přístupových sítí. 8
1.2 Obecné schéma optické přístupové sítě. 9
2.1 Evoluce systémů PON založených na časovém dělení TDM 11
2.2 Princip přenosu TDM-PON v sestupném směru. 12
2.3 Princip přenosu TDM-PON ve vzestupném směru. 13
2.4 Topologie PON. 13
2.5 Struktura rámce GTC v sestupném směru. 17
2.6 Struktura rámce GTC ve vzestupném směru. 18
2.7 Struktura rámce GEM. 19
2.8 Proces generování a výměny šifrovacího klíče v systémech GPON. 20
2.9 Pásma vlnových délek pro GPON, XG-PON a služby TV vysílání. 22
2.10 Struktura rámce XGTC v sestupném směru. 23
2.11 Struktura rámce XGTC ve vzestupném směru. 23
2.12 Struktura rámce XGEM. 24
2.13 Bezpečnostní model XG-PON. 25
2.14 Derivace bezpečnostních klíčů v XG-PON. 27
2.15 Struktura multirámce architektury EPON v sestupném směru. 28
2.16 Struktura multirámce architektury EPON ve vzestupném směru. 29
2.17 Struktura rámce Ethernet v architektuře EPON. 29
2.18 Pásma vlnových délek pro EPON, 10GEPON a služby TV vysílání. 30
3.1 Kanály CWDM definované v ITU-T G.694.2. 33
3.2 WDM-PON s pevně přidělenými vlnovými délkami. 34
3.3 WDM-PON s vydělováním délek pomocí odbočnice AWG. 35
3.4 WDM-PON s kaskádním zapojením rozbočovače a odbočnic AWG. 35
3.5 Hybridní WDM/TDM-PON. 36
3.6 WDM-PON s využitím laserů Fabry-Perot. 37
3.7 Princip vydělování vlnových délek odbočnicí AWG. [17] 37
4.1 Obecný algoritmus kryptografie. 41
4.2 Algoritmus symetrického šifrování. 42
4.3 Operace SubBytes. 43
4.4 Operace ShiftRows. 43
4.5 Operace MixColumns. 44
4.6 Operace AddRoundKey. 44
4.7 Algoritmus asymetrického šifrováni. 45
4.8 Struktura přenášeného bloku. 46

4.9 Model autentizace IEEE 802.1x. 48
5.1 LG-Nortel EAST 1100. 51
5.2 LG-Nortel WPF 1132c. 51
5.3 LG-Nortel EARU 1112. 52
5.4 EXFO FTB-400. 52
5.5 Přihlašovací okno EA Manageru. 53
5.6 Úvodní okno EA Manageru. 54
5.7 Okno se zásuvnými kartami (Equipment View). 54
5.8 Okno s možností aktivace a deaktivace koncových jednotek (Facility). . . 55
5.9 Topologie č. 1. 55
5.10 Spektrum kanálu č. 2 před a po aktivaci jednotky na kanálu č. 1. 56
5.11 Topologie č. 2. 57
5.12 Spektrum naměřené na jednotce ONU připojené na kanálu č. 7. 58
5.13 Topologie č.1 v prostředí Optiwave. 59
5.14 Spektrum před filtrem AWG. 59
5.15 Spektrum za filtrem AWG na jednotce ONU 2. 60
5.16 Topologie pro simulaci reálné situace. 60
5.17 Optické spektrum na výstupu sdružovače. 61
5.18 Diagram oka jednotky ONU 2. 62
5.19 Topologie pro simulaci odposlechu s využitím přeslechu. 62
5.20 Odfiltrovaný signál na vlnové délce 1578,482 nm. 63
5.21 Odfiltrovaný a zesílený signál na vlnové délce 1578,482 nm. 63
5.22 Diagram oka zesíleného signálu. 64
A.1 Spektrum kanálu č. 7 před a po aktivaci jednotky na kanálu č. 6. . . . . A-I
A.2 Spektrum kanálu č. 9 před a po aktivaci jednotky na kanálu č. 8. . . . . A-II
A.3 Spektrum kanálu č. 9 před a po aktivaci jednotky na kanálu č. 10. . . . . A-III
A.4 Spektrum kanálu č. 20 před a po aktivaci jednotky na kanálu č. 21. . . . . A-IV
A.5 Spektrum kanálu č. 28 před a po aktivaci jednotky na kanálu č. 27. . . . . A-V
A.6 Spektrum kanálu č. 31 před a po aktivaci jednotky na kanálu č. 32. . . . . A-VI
B.1 Hlavní rozvaděč N311. . . . . B-I
C.1 Schéma topologie č. 1 v Optiwave. . . . . C-I
C.2 Schéma topologie pro simulaci odposlechu s využitím přeslechu v Optiwave.C-II

Úvod

Trendem posledních let se v oblasti telekomunikačních sítí stalo nasazování optických sítí namísto původních systémů vystavěných na metalických vedeních. Výjimkou nejsou ani přístupové sítě, kde stále více poskytovatelů internetových služeb uvádí do provozu pasivní optické sítě PON (Passive Optical Network). Protože se počet těchto sítí stále zvyšuje a zvyšuje se i počet připojených koncových uživatelů k těmto sítím, je nezbytně nutné zajistit jejich bezpečný provoz.

Tématem této bakalářské práce je bezpečnost a bezpečnostní rizika pasivních optických sítí nejen současné generace, ale i nové generace, především technologie WDM-PON.

V úvodní kapitole jsou představeny optické přístupové sítě, jejich dělení a metody využívané k přenosu. Aby bylo možné odhalit původ a závažnost bezpečnostních rizik, je nutné se detailně seznámit s principy přenosu, strukturou přenášených dat a bezpečnostními mechanismy jednotlivých technologií PON. Tímto se zabývají kapitoly 2 a 3. Další kapitola se věnuje bezpečnosti sítí PON obecně. Jsou zde popsána zjištěná bezpečnostní rizika obou generací optických pasivních sítí a detailně jsou rozebrány bezpečnostní mechanismy používané k jejich zamezení.

Cílem praktické části této práce, popsané v kapitole 5, je ověření bezpečnostních rizik spojených s provozem technologie nové generace, WDM-PON. Tato rizika jsou otestována nejen v laboratorních podmínkách, ale i v simulačním prostředí Optiwave.

1 Optické přístupové sítě

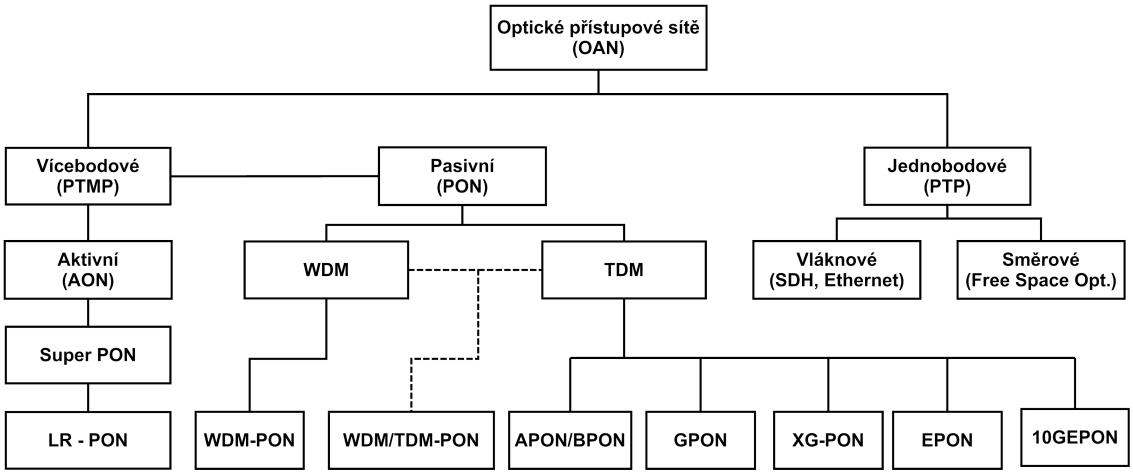
Za přístupovou síť je považována ta část telekomunikační sítě, která spojuje koncové zákazníky s jejich poskytovatelem internetových služeb. Nejedná se tedy o páteřní, ani o lokální sítě, ale o sítě středního dosahu v řádech stovek metrů až po desítky kilometrů.

S rostoucím portfoliem služeb a jejich zvýšených požadavků na šířku pásma, stejně tak se zvyšujícím se počtem připojených uživatelů dochází k ústupu technologií vystavěných na metalických vedeních (ADSL, VDSL, ISDN, HDSL a další), které tyto požadavky už nejsou schopny naplnit. Do popředí zájmů většiny poskytovatelů síťových služeb se jako náhrada dostávají optické sítě. Po vytlačení metalických systémů postupně z páteřních, transportních, metropolitních a nyní i přístupových sítí, zůstávají poslední dominantou metalických systémů už pouze lokální sítě LAN (Local Area Network), kde je v současné době nasazení optických systémů ekonomicky neefektivní.

Přenosovým mediem, použitým v optických sítích, je jak napovídá název optické vlákno, které oproti ostatním typů přenosových medií nabízí několik výhod. Především se jedná o velkou šířku pásma a s ní spojenou vysokou přenosovou rychlost. Dále jsou optická vlákna imunní proti elektromagnetickému rušení, mají menší útlum přenášeného signálu a poskytují větší bezpečnost proti odposlechu [1].

1.1 Dělení optických přístupových sítí

Optické přístupové sítě OAN (Optical Access Networks) jsou rozděleny do dvou základních skupin. Pasivní optické sítě PON (Passive Optical Network), které nevyužívají v distribučních částech přístupových sítí aktivní prvky a aktivní optické sítě AON (Active Optical Network), které aktivní prvky, např. opakovače a zesilovače využívají. Základní rozdělení optických přístupových sítí je vyobrazeno na obrázku 1.1.



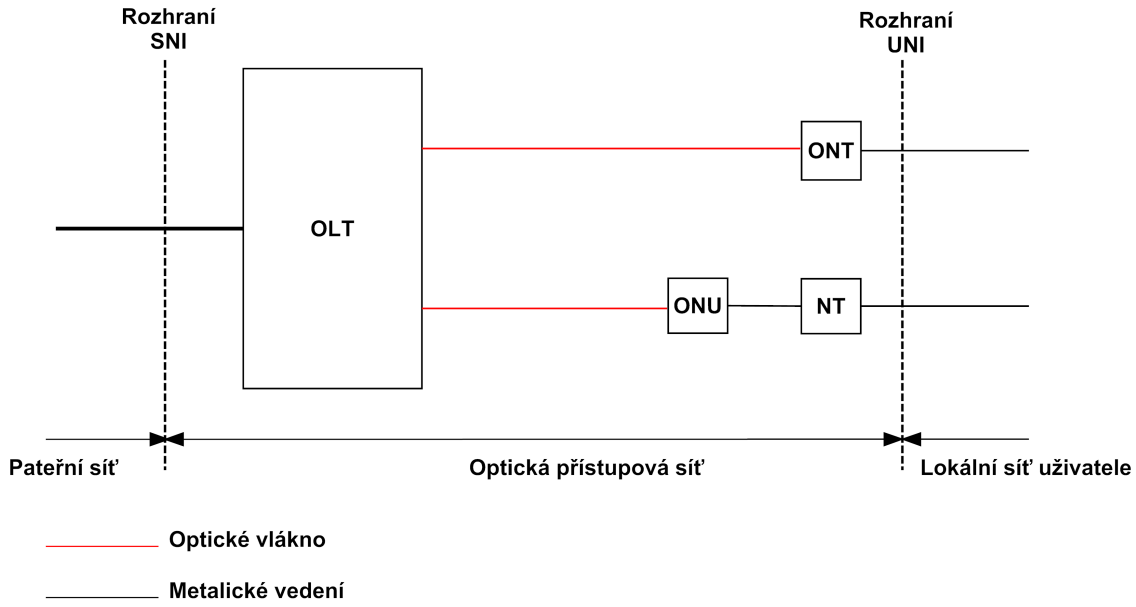
Obrázek 1.1: Rozdělení optických přístupových sítí.

1.2 Funkční celky optické přístupové sítě

Obecné schéma optických přístupových sítí zobrazuje obrázek 1.2. Základními prvky pro realizaci optické přístupové sítě jsou [2]:

- **optická distribuční síť ODN (Optical Distribution Network)**, soubor přenosových prostředků nacházejících se mezi optickým linkovým zakončením OLT a síťovými jednotkami a optickými síťovými zakončeními ONU, ONT. Jedná se o fyzické prvky sítě, jako jsou např. optická vlákna, pasivní optické rozbočovače, konektory, spojky, svary a vlnové filtry,
- **optické linkové zakončení OLT (Optical Line Termination)**, zařízení nacházející se na rozhraní páteřní a přístupové sítě, které ukončuje distribuční síť na straně poskytovatele připojení. Jelikož v PON sítích může být použito několik různých protokolů, které se mohou lišit od protokolů použitých v páteřní síti, je jednou z hlavních úloh této jednotky konverze mezi těmito protokoly. Další, neméně důležitou funkcí je řízení přístupové sítě, tzn. správa optických koncových zakončení a síťových jednotek ONT a ONU,
- **optické síťové zakončení ONT (Optical Network Terminal)**, zařízení na straně účastníka, které má na starost převod optického signálu z optické distribuční sítě na signál elektrický, který zpracovávají koncová zařízení uživatele,
- **optická síťová jednotka ONU (Optical Network Unit)**, zařízení na straně účastníka se stejnou úlohou jako ONT. Rozdíl spočívá v dalším šíření, teď už elektric-

kého signálu skrze metalická vedení, případně bezdrátově pomocí technologie Wi-Fi. Jednotka ONU tedy umožňuje připojení více uživatelů.



Obrázek 1.2: Obecné schéma optické přístupové sítě.

1.3 Uspořádání FTTx

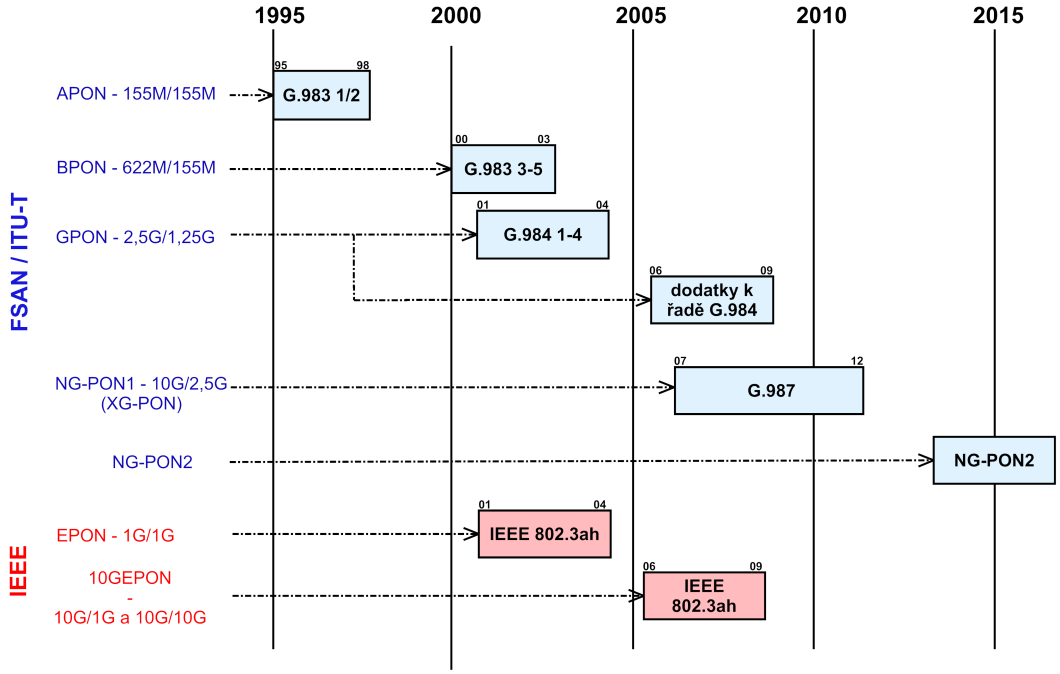
Optické sítě bývají označovány zkratkou FTTx (Fiber To The x), kde x určuje bod, ve kterém bude ukončena optická síť, respektive vzdálenost kam až povede optické vlákno a odkud bude pokračovat metalické vedení. Je to obecný pojem pro všechny širokopásmové síťové architektury, využívající optická vlákna jako náhradu za metalická vedení. Tento pojem vznikl jako zobecnění několika konfigurací nasazení (FTTN, FTTC, FTTB, FTTH a další). Systémy FTTx mohou reprezentovat spojení typu bod-více bodů P2MP (Point to Multipoint) i bod-bod P2P (Point to Point). Nejčastěji se můžeme setkat s těmito typy konfigurací [2], [3]:

- **FTTH (Fiber To The Home)**, optické vlákno je přivedeno až do obytného prostoru koncového zákazníka. Další šíření konektivity (např. LAN) je v režii zákazníka,
- **FTTB (Fiber To The Building)**, optické vlákno je přivedeno do budovy, kde se konektivita dále šíří metalickými rozvody, případně bezdrátově technologií Wi-Fi celou budovou. Tento systém se podobá systému FTTH, ale slouží k připojení většího počtu uživatelů,

- **FTTC (Fiber To The Curb)**, optické vlákno je přivedeno do rozvaděče, který se obvykle nachází před blokem budov, do kterých má být připojení přivedeno. Z rozvaděče je signál šířen pomocí metalických vedení,
- **FTTN (Fiber To The Node)**, optické vlákno je ukončeno v rozvaděči, k němuž jsou uživatelé připojeni přípojkami xDSL (nejčastěji VDSL, ADSL, SHDSL). Řešení je velmi podobné systému FTTC, rozvaděč se v tomto případě ale nachází ve větší vzdálenosti od koncových uživatelů,
- **FTTP (Fiber To The Premises)**, jedná se o společné označení systémů FTTB a FTTH. Označuje přivedení optického vlákna do budovy účastníka a nerozlišuje další šíření konektivity,
- **FTTO (Fiber To The Office)**, optické vlákno je přivedeno opět jako v případě FTTH až k zákazníkovi. Tento systém je ale určen pro komerční použití zákazníkům s velkými požadavky na přenosovou kapacitu, např. banky, úřady, firemní společnosti.

2 Technologie TDM-PON

Většina v současnosti nasazovaných systémů PON spadá do kategorie sítí s časovým sdružováním, označované jako TDM-PON (Time Division Multiplexing Passive Optical Network). Jedná se o technologie APON (ATM-PON), BPON (Broadband PON), GPON (Gigabit PON), sítě nové generace NG-PON (XG-PON1, 2), EPON (Ethernet PON) a 10GEPON (10 Gbit/s Ethernet PON). Podrobně jsou tyto technologie popsány v kapitole 2. Systémy se od sebe liší především použitými přenosovými protokoly, šířkou pásma, kapacitou a zabezpečením. Časový vývoj technologií TDM-PON je zachycen na obrázku 2.1.



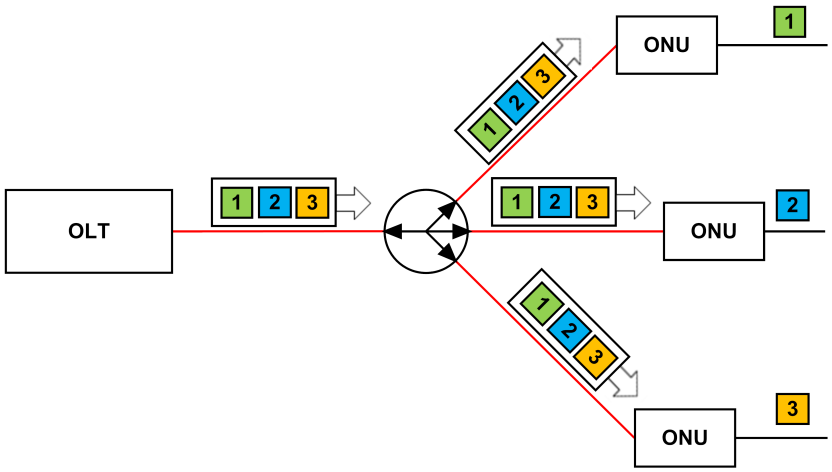
Obrázek 2.1: Evoluce systémů PON založených na multiplexu časového dělení TDM[1]

APON, BPON, GPON a NG-PON architektury jsou vyvíjeny skupinou FSAN (Full Service Access Network), sdružením poskytovatelů síťových služeb a výrobců telekomunikační techniky. Tyto architektury se při přenosu spoléhají na rámcové struktury s velmi přesným časováním a synchronizací a jejich detailní specifikace jsou vydávány v rámci série doporučení mezinárodní společnosti pro standardizaci telekomunikací ITU-T (Telecommunication Standardization Sector of the International Telecommunications Union).

[1] Uvedené rychlosti odpovídají původním verzím jednotlivých doporučení.

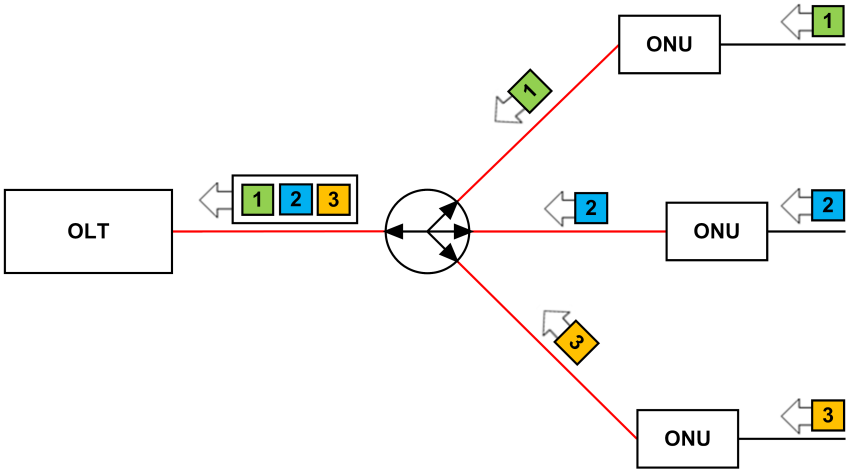
Architektury EPON a 10G-EPON jsou standardizovány institutem IEEE (Institute of Electrical and Electronics Engineers) a primárně se zaměřují na zachování architektonického modelu Ethernet. V systémech EPON neexistují žádné explicitní rámcové struktury s přesným časováním jako je tomu u architektur pod hlavičkou ITU-T. Jednotlivé Ethernet rámce jsou přenášeny v dávkovém režimu s využitím bitových prodlev mezi jednotlivými rámci [6].

Systémy TDM-PON využívají k rozdělování signálu mezi více účastníků pasivní optický rozbočovač označovaný též splitter. Tento prvek pouze zkopíruje tok dat přicházející z jednotky OLT na všechny koncové jednotky a zakončení ONU, ONT. Koncové jednotky rozpoznají jim určená data podle adresních štítků obsažených v signálu. Tyto data následně přijmou a data určená ostatním jednotkám zahodí. Tento princip je vyobrazen na obrázku 2.2.



Obrázek 2.2: Princip přenosu TDM-PON v sestupném směru.

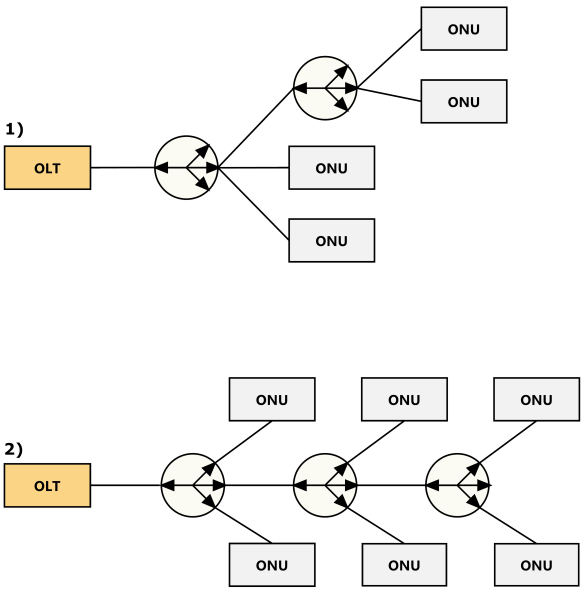
Ve vzestupném směru má každá jednotka ONU, ONT od jednotky OLT vyhrazený přesný časový interval ve kterém může vysílat tak, aby nedošlo k překrývání nebo kolizi s vysíláním jiných jednotek, viz obrázek 2.3 [2].



Obrázek 2.3: Princip přenosu TDM-PON ve vzestupném směru.

2.1 Topologie PON

Topologie používané v systémech PON jsou totožné s topologiemi používanými v běžných telekomunikačních sítích. Jednotlivé topologie zobrazuje obrázek 2.4. Topologie stromová (1) je nejpoužívanější. Sběrnicová topologie (2) zvětšuje rozestupy mezi koncovými jednotkami, proto se obvykle používá v odlehlých oblastech s velkými vzdálenostmi mezi účastníky. [7].



Obrázek 2.4: Topologie PON.

2.2 APON/BPON (ITU-T G.983)

APON (ATM-PON) a BPON (Broadband PON) jsou rozdílné názvy TDM-PON architektury vydané v rámci doporučení řady ITU-T G.983 v roce 1998. Zatímco název BPON je používán spíše z marketingových důvodů, APON přesně vyjadřuje povahu přenosu, a sice že jsou v tomto standardu pro přenos použity buňky protokolu ATM (Asynchronous Transfer Mode).[2]

Rychlost přenosu v systémech APON byla specifikována pro symetrický i asymetrický režim. V symetrickém režimu je rychlost v obou směrech 155,52 Mbit/s. V asymetrickém režimu 622,08 Mbit/s ve směru sestupném (downstream) a 155,52 Mbit/s ve směru vzestupném (upstream). Aktualizovaná verze doporučení ITU-T G.983 z roku 2005 specifikuje rychlost ve směru sestupném až 1244,16 Mbit/s. Všechny varianty rychlostí jsou uvedeny v tabulce 2.1.

Tabulka 2.1: Varianty rychlostí technologie APON/BPON.

Downstream (Mbit/s)	Upstream (Mbit/s)
155,52	155,52
622,08	155,52
622,08	622,08
1244,16	155,52
1244,16	622,08

Technologie APON umožňuje připojení až 16 koncových jednotek s maximálním dosahem 20 km. Tyto dva údaje se odvíjí od velikosti vložného útlumu v síti. Útlum se zvyšuje s počtem připojených jednotek, pasivních rozbočovačů, konektorů a podobně. Pro všechny standardy ITU-T jsou definovány 3 útlumové třídy, které jsou popsány v doporučení ITU-T G.982.

- třída A: 5–20 dB
- třída B: 10–25 dB
- třída C: 15–30 dB

Obousměrný provoz je v APON systémech řešen použitím vlnového multiplexu WDM (Wavelength Division Multiplexing) tedy na jednom optickém vlákně jsou přenášeny dvě

[2] ATM je telekomunikační koncept, který vznikl v 80. letech 20. století, definovaný standardy pro přenos celého spektra uživatelského provozu, zahrnující hlasové, datové a video signály.

vlnové délky. Pro sestupný směr je použita vlnová délka z pásma 1480–1500 nm a pro směr vzestupný z pásma 1260–1360 nm. Možné je pro obousměrný provoz také použíti dvou oddělených optických vláken, kdy jedno je použito pro vzestupný a druhé pro sestupný směr. V tomto případě obě vlákna pracují s vlnovou délkou 1310 nm [3].

2.2.1 Zabezpečení APON

V systémech APON jsou zabezpečena pouze uživatelská data v sestupném směru. K šifrování je použita metoda Churning viz kapitola 4.3.1. Kromě toho tyto systémy podporují typ autentizace založený na výměně hesel popsaný v kapitole 4.5.1 [8].

2.3 GPON (ITU-T G.984)

GPON (Gigabit-capable PON) je nástupcem technologie APON/BPON. Standardizována tato technologie byla v rámci doporučení ITU-T G.984 v roce 2003. Největší změnu představuje nasazení nového protokolu GEM (GPON Encapsulation Method) na druhé vrstvě GTC (GPON Transmission Convergence Layer) referenčního modelu a zavedení nového systému služebních zpráv a řízení OMCI (ONU Managment and Control Interface). V původní verzi doporučení ITU-T G.984.3 z roku 2004 měla vrstva GTC rovněž režim podporující přenos protokolu ATM. Tento přenos byl zděděn z technologie APON/BPON a měl sloužit k částečné zpětné kompatibilitě s některými, koncovými jednotkami této technologie. Ukázalo se ale, že kompatibilita jednotlivých zařízení je problematická a v praxi se ji využívalo jen minimálně, jestli vůbec. Toto v kombinaci s celkovým úpadkem technologií postavených na ATM vedlo k tomu, že byla podpora přenosu protokolu ATM v aktualizované verzi doporučení z roku 2008 z popisu vlastností GTC vrstvy odstraněna [9].

GPON nabízí několik variant přenosových rychlostí, viz tabulka 2.2. Obvykle se používá asymetrický režim s rychlostí 2488,32 Mbit/s ve směru sestupném a 1244,16 Mbit/s ve směru vzestupném.

Obousměrný provoz je opět řešen použitím vlnového multiplexu, došlo ale k úpravě vlnových pásem. Pro provoz na jednom optickém vlákně byla v sestupném směru zvolena vlnová délka z pásma 1480–1500 nm a ve vzestupném směru z pásma 1290–1330 nm. Kromě zvýšené přenosové rychlosti, nabízí technologie GPON v porovnání s APON větší dělící poměr, umožňující připojení až 64 koncových jednotek [2], [9].

Tabulka 2.2: Varianty rychlostí technologie GPON.

Downstream (Mbit/s)	Upstream (Mbit/s)
1244,16	155,52
1244,16	622,08
1244,16	1244,16
2488,32	155,52
2488,32	622,08
2488,32	1244,16
2488,32	2488,32

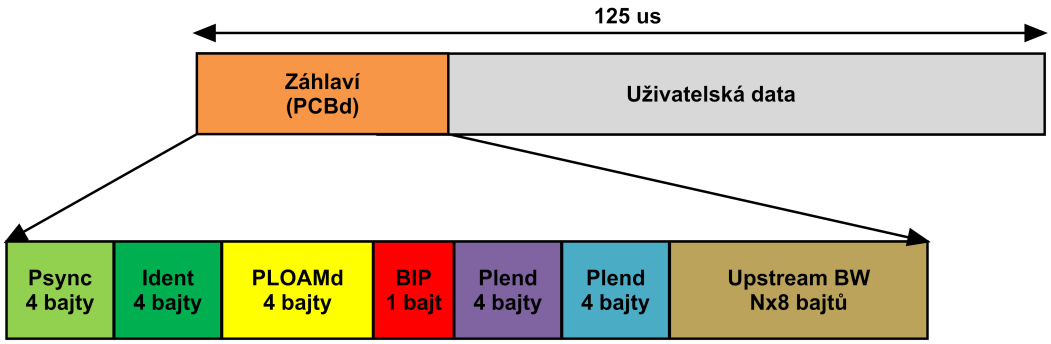
2.3.1 Přenos v GPON

Doporučení ITU-T G.984.3 popisuje vrstvu GTC, což je ekvivalent spojové vrstvy v referenčním OSI modelu. Hlavní úlohou této vrstvy je multiplexování a demultiplexování přenosu mezi OLT a ONU jednotkou a ovládání přístupu k médiu MAC (Media Access Control). Dříve tato vrstva podporovala tři režimy přenosu, přenos GEM rámců, přenos ATM buněk a kombinaci obou současně. Jak bylo ale zmíněno výše, přenos ATM buněk se již nevyužívá, byl z doporučení odstraněn a k přenosu tak slouží pouze GEM rámce

Jednotlivé GEM rámce jsou zapouzdřeny do přenosových GTC rámců, viz obrázky 2.5 a 2.6. Tyto rámce mají v sestupném směru pevně stanovenou délku 125 μs pro obě přenosové rychlosti. Při přenosové rychlosti 1244,16 Mbit/s je velikost jednoho GTC rámce 19440 bajtů, při dvojnásobné rychlosti 2488,32 Mbit/s je i velikost rámce dvojnásobná, tedy 38880 bajtů. Kromě přenášených rámců GEM s uživatelskými daty, obsahuje rámec GTC i záhlaví PCBd (Physical Control Block downstream), jehož délka je shodná pro obě rychlosti a odvíjí se od počtu připojených ONU jednotek.
Záhlaví PCBd obsahuje tyto bloky [2], [9]:

- **synchronizační pole Psync (Physical synchronization)**, obsahující posloupnost 32 bitů, kterou začíná každé PCBd záhlaví. Slouží ONU jednotce k detekci počátku rámce a k odvození synchronizace sestupného směru,
- **identifikační pole Ident (Ident field)**, o velikosti 32 bitů. První bit pole indikuje, zdali je v přenosu použito kódování FEC (Forward Error Correction). Druhý bit slouží jako rezerva pro pozdější použití. Zbývajících 30 bitů slouží k číslování rámců, tyto bity obsahují čítač, který se s každým dalším odeslaným GTC rámcem zvyšuje o jednotku. Pokud čítač dosáhne maximální hodnoty, je v následujícím rámci nastaven zpět na nulu a číslování začíná od znova,

- **pole PLOAMd (PLOAM downstream field)**, o velikosti 13 bajtů sloužící k přenosu zpráv PLOAM (Physical Layer OAM), obsahujících řízení operací fyzické vrstvy. Protože jedna zpráva zabere celou velikost pole, může být v každém poli odeslána pouze jedna tato zpráva,
- **pole bitově prokládané parity BIP (BIP field)**, o velikosti 8 bitů, sloužící k indikaci chyb v PCBd záhlaví,
- **pole PLend (PLend Field)**, o velikosti 32 bitů. Prvních 12 bitů obsahuje informace o délce posledního bloku PCBd záhlaví. Dalších 12 bitů původně neslo informace o délce ATM části uživatelských dat, ale jelikož byla podpora ATM z doporučení odstraněna, nabývají tyto bity nulové hodnoty. Posledních 8 bitů zabírá CRC součet. Pro větší odolnost vůči chybám přenosu je toto pole odesláno dvakrát,
- **pole US Bwmap (Upstream BandWidth map)**, tvořené 8 bajtovými záznamy, jejichž počet udává pole PLend. Záznamy nesou informace o přidělené vysílací kapacitě ve vzestupném směru jednotlivým ONU jednotkám v síti.

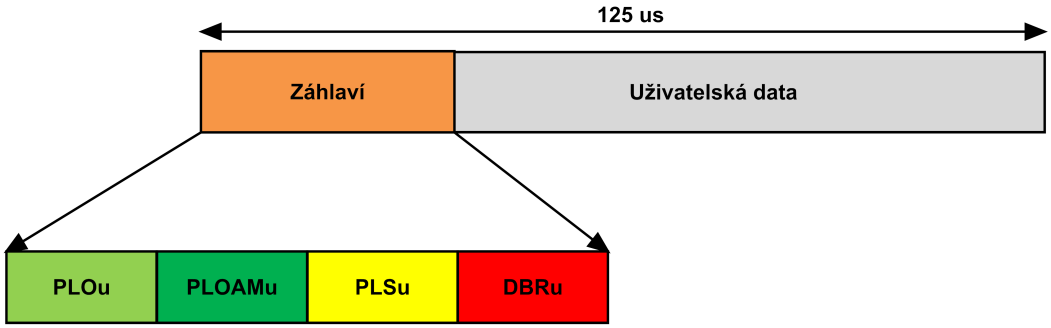


Obrázek 2.5: Struktura rámce GTC v sestupném směru.

Po záhlaví PCBd následuje v GTC rámci blok s uživatelskými daty, která jsou začleněna do struktury definované GEM protokolem, takzvaného GEM rámce.

Ve vzestupném směru je délka GTC rámců opět 125 μs a jejich obsah tvoří data vysílaná z jednotlivých koncových jednotek. Struktura rámce je totožná se strukturou rámce v sestupném směru a opět se tedy skládá ze záhlaví a uživatelských dat. Povinnou částí záhlaví je pouze pole PLOu (Physical Layer Overhead upstream), zbývající tři části jsou odesílány podle požadavků jednotky OLT. Záhlaví může být tvořeno kombinací těchto polí [2], [9]:

- **PLOu**, obsahující preambuli sloužící k synchronizaci jednotek OLT a ONU, delimiter označující začátek upstream přenosu, bitovou paritu BIP pro zabezpečení přenosu preambule a delimiteru vůči chybám, pole ONU-ID s identifikátorem koncové jednotky a indikační pole IND poskytující informace o počtu uživatelských dat čekajících na odeslání a jejich prioritě,
- **PLOAMu (PLOAM upstream field)**, sloužící k přenosu zpráv PLOAM , struktura je totožná s polem PLOAMd v sestupném směru,
- **PLSu (Power Levelling Sequence Upstream)**, v původní verzi doporučení mělo toto pole sloužit jednotce ONU ke korekci a nastavení vysílací úrovně, v aktuální verzi doporučení jsou bity tohoto pole nulovány,
- **DBRu (Dynamic Bandwidth Report Upstream)**, sloužící k odeslání požadavku o přidělení vysílací kapacity.



Obrázek 2.6: Struktura rámce GTC ve vzestupném směru.

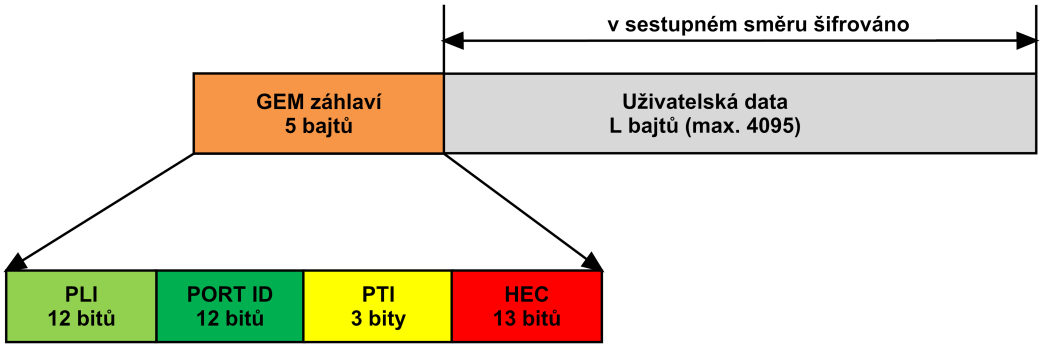
Samotná uživatelská data jsou stejně jako v případě rámce GTC v sestupném směru začleněna do rámce GEM, viz obrázek 2.7.

Rámec GEM se skládá ze záhlaví o pevné velikosti 5 bajtů a uživatelských dat s proměnlivou délkou 0–4095 bajtů. V sestupném směru jsou tato data šifrována. Hlavní výhoda GEM protokolu oproti přenosu ATM buněk spočívá ve flexibilnější práci s uživatelskými daty a umožnění manipulace s různými typy těchto dat, vhodný je například pro přenos Ethernet rámců.

Záhlaví rámce GEM je tvořeno těmito bloky [2], [9]:

- **PLI (Payload Length Indicator)**, pole velikosti 12 bitů, určuje v bajtech velikost přenášených dat následujících za záhlavím GEM,

- **Port-ID (Port Identificator)**, pole o velikosti 12 bitů, sloužící k přidělení unikátního čísla portu, na který jsou uživatelská data odeslána, respektive ze kterého byla odeslána,
- **PTI (Payload Type Indicator)**, posloupnost 3 bitů, podle které se určí, o jaký typ přenášených dat se jedná. Zda se jedná o začátek nebo konec rámce úseku uživatelských dat,
- **HEC (Header Error Detection and Correction)**, pole o velikosti 13 bitů, sloužící k zabezpečení přenosu záhlaví GEM , poskytuje detekci a opravu chyb. K tomuto účelu je použito kódování BHC (39, 12, 2) v kombinaci s bitovou paritou.

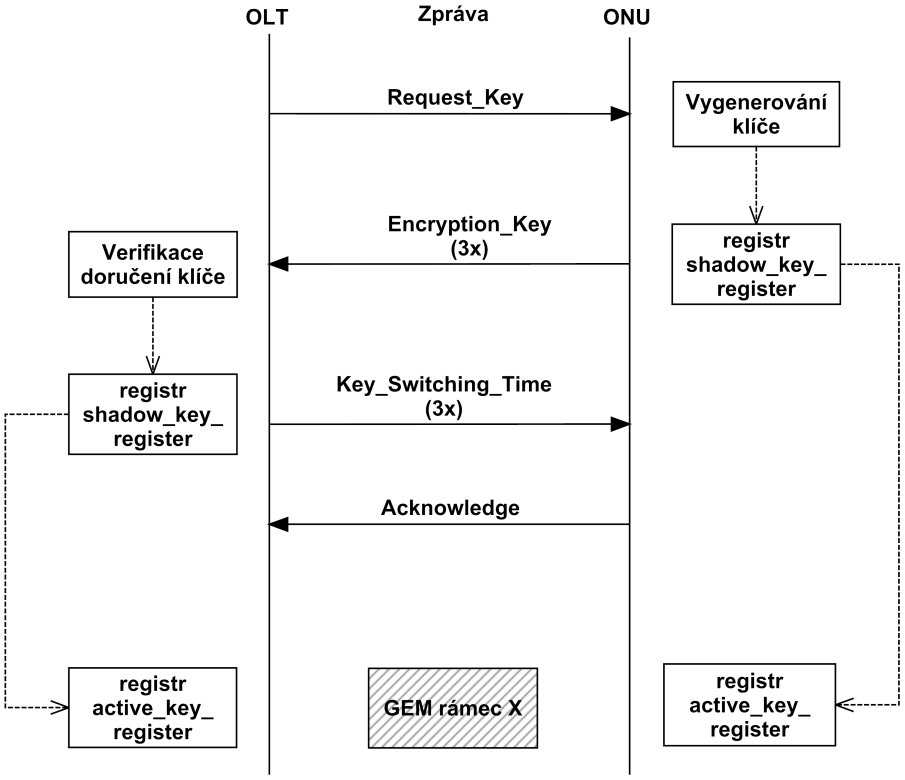


Obrázek 2.7: Struktura rámce GEM.

2.3.2 Zabezpečení GPON

K šifrování přenosu dat je použita šifra AES s klíčem o délce 128 bitů viz kapitola 4.3.2. Proces generování a výměny šifrovacího klíče je znázorněn na obrázku 2.8. Šifrovací klíč vytváří jednotka ONU po obdržení žádosti Request_Key ze strany jednotky OLT. Po vytvoření klíče si jednotka ONU klíč uloží do registru shadow_key_register a následně jej odešle jednotce OLT formou PLOAM zprávy Encryption_Key. Protože je velikost klíče větší než maximální velikost této zprávy, je klíč rozdělen na dvě části. Pro zajištění korektního doručení jsou obě části klíče odeslány třikrát. Pokud jednotka OLT neobdrží tři shodné klíče, vyšle novou žádost Request_key. Pokud doručení klíče proběhlo úspěšně, uloží si jednotka OLT klíč do svého registru shadow_key_register a odešle jednotce ONU zprávu Key_Switching_time, ve které informuje o číslu prvního rámce X, na který se daný šifrovací klíč aplikuje. Tato zpráva je opět odeslána třikrát, ale stačí potvrzení přijetí alespoň jedné z nich. Na začátku daného rámce X si jednotky OLT i ONU zkopírují

obsah registru shadow_key_register do registru active_key_register, čímž se zajistí vzájemná synchronizace klíčů na obou stranách.



Obrázek 2.8: Proces generování a výměny šifrovacího klíče v systémech GPON.

Šifrovány jsou opět pouze samotná uživatelská data v sestupném směru. Přenos záhlaví jednotlivých zpráv, služebních zpráv a komunikace ve vzestupném směru, včetně přenosu šifrovacího klíče, zůstal beze změny, nezabezpečen. Povinnou součástí systémů GPON je rovněž implementace autentizace a opravného kódování FEC (Forward Error Correction), sloužícího k detekci a opravě chyb vzniklých při přenosu. K tomu účelu je použito kódování Reed – Solomon RS(255,239) [9].

2.4 XG-PON (ITU-T G.987)

Po ukončení standardizace technologie GPON započala vývojová FSAN (Full Service Access Network) skupina ve spoluprací s ITU-T práci na nové deseti gigabitové technologii.

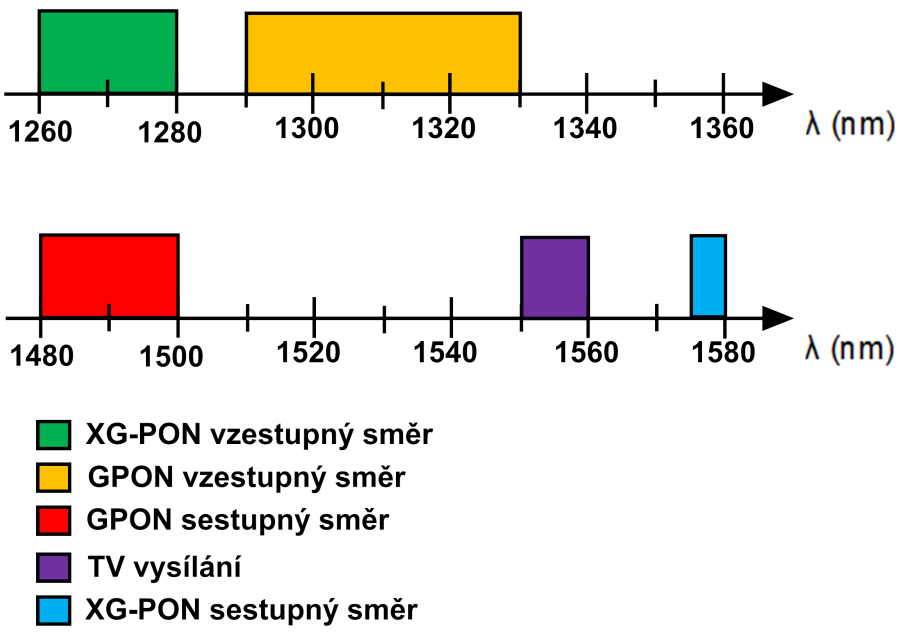
Vývoj směrem k této technologii započal v roce 2006 vydáním doporučení ITU-T G.984.5, jehož cílem bylo usnadnit přechod ze stávajících GPON systémů. Doporučení definuje vlnové rozsahy, které by bylo možné použít pro budoucí technologie a blo-

kující filtry v koncových jednotkách, které by zabránily přeslechům mezi vlnovými délkami technologií GPON a systémů nové generace Next Generation PON (NG-PON) [10].

Ke konci roku 2007 byl vývoj zaměřen na definování úplně nového systému, ale protože bylo mnoho kandidátů (TDM-PON, WDM-PON, CDMA-PON a další) jejichž architektura byla navzájem velmi odlišná a výrazně se lišil i jejich profil služeb, bylo obtížné tyto technologie objektivně porovnat a vybrat z nich nejlepší variantu. Z tohoto důvodu byl vývoj NG-PON systémů rozdělen do dvou skupin. První skupina NG-PON1 se zaměřila na PON technologie, které by byly kompatibilní se systémy GPON a při jejichž nasazení by byla zachována stávající optická distribuční síť ODN. Druhá skupina NG-PON2 zahrnovala všechny ostatní systémy, které k zprovoznění potřebovaly buď to změnu v ODN nebo technologie, které ještě nebyly v požadovaném časovém horizontu, nejen z finančních důvodů k dispozici.

Počátkem roku 2008 měla skupina FSAN shromážděných několik variant možných systémů pro NG-PON1. Z těchto navrhnutých systému bylo potřeba na základě jejich výhod a nevýhod vybrat jednu, která by nejlépe odpovídala požadavkům na nízkou cenu, při co nejvyšší míře spolehlivosti. Některé systémy byly vyřazeny, protože nesplňovaly požadavek na zachování ODN. Jiné byly vyřazeny, protože byly až příliš inovativní a byla s nimi spojena velká technická rizika, jednalo se například o hybridní systémy DWDM/XG-PON. Další byly vyřazeny, protože byly naopak až příliš málo inovativní, například systém, ve kterém měly být použity čtyři vlnové délky ve směru sestupném a jedna vlnová délka ve směru vzestupném s asymetrickou rychlostí 10/1,25 Gbit/s. Posledním vyřazeným kandidátem se stal systém XG-PON2 se symetrickou rychlostí 10 Gbit/s, u kterého panovaly obavy z vysoké pořizovací ceny.

Nejlepší variantou se tak po všech úvahách stal pro skupinu FSAN systém XG-PON1 s jednou vlnovou délkou v každém směru a asymetrickou rychlostí 10 Gbit/s ve směru sestupném a 2,5 Gbit/s ve směru vzestupném. Aby byl zachován požadavek na vzájemnou koexistenci se systémy GPON, bylo potřeba zvolit pásma vlnových délek tak, aby se s těmito systémy nepřekrývala. Zvolená pásma znázorňuje obrázek 2.9. Pro směr sestupný je použita vlnová délka z pásma 1575–1580 nm a pro směr vzestupný z pásma 1260–1280 nm [10].

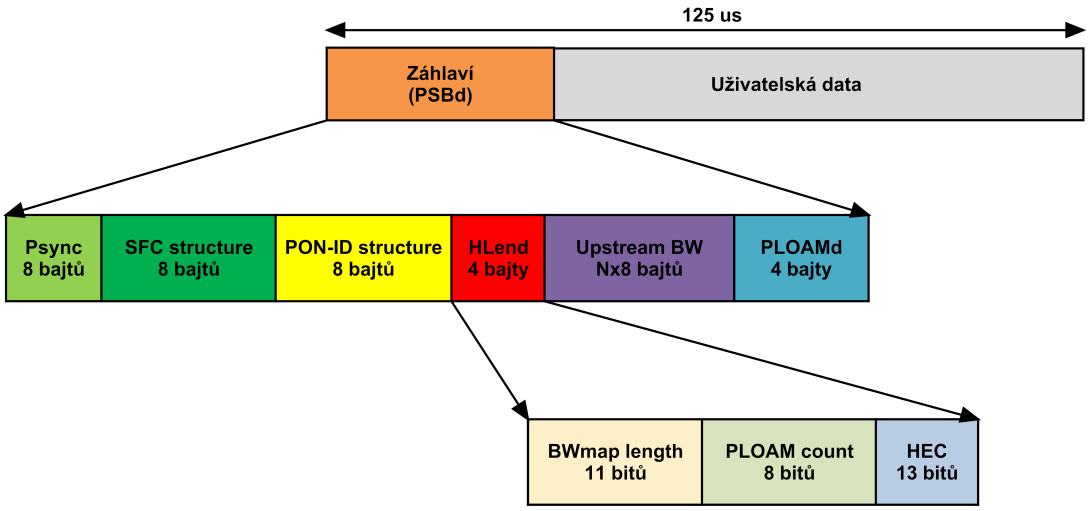


Obrázek 2.9: Pásma vlnových délek pro GPON, XG-PON a služby TV vysílání.

2.4.1 Přenos v XG-PON

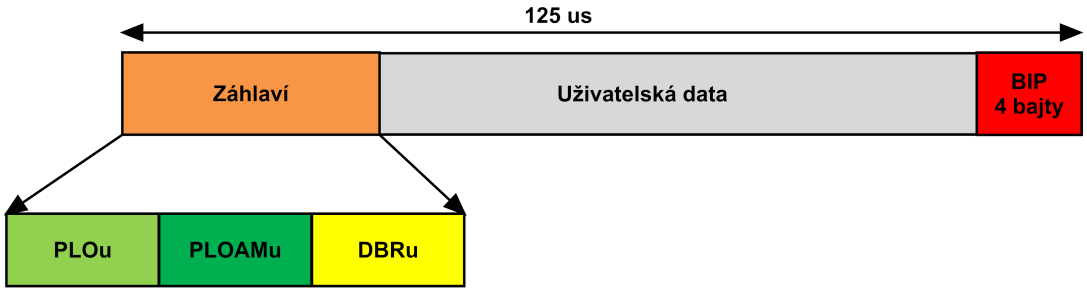
Systémy XG-PON používají k přenosu rámce XGTC (XG-PON Transmission Convergence Layer), viz obrázky 2.10 a 2.11. Tyto rámce jsou strukturou velmi podobné rámcům GTC, avšak doznaly pár změn tak, aby byly schopny zaštítit zvýšené požadavky spojené například s vyšším celkovým počtem připojených koncových jednotek. Rámce XGTC mají opět přesně stanovenou délku 125 μs a v obou směrech se skládají ze záhlaví a bloku uživatelských dat.

V sestupném směru začíná rámec záhlavím PSBd (Physical Synchronization Block downstream). Pole SFC structure je ekvivalentem pole Ident a jeho význam je popsán, stejně jako u polí PSync, HLend (PLend), US BWmap a PLOAMd v kapitole 2.3.1. Novým prvkem je pole PON-ID structure jehož hodnota je určená OLT jednotkou a slouží k identifikaci konkrétního PON signálu. Pole PLOAM count udává počet zpráv PLOAM, pole BWmap length udává počet struktur v poli BWmap a pole Hybrid Error Correction (HEC) zajišťuje detekci a korekci chyb v záhlaví rámce [11].



Obrázek 2.10: Struktura rámce XGTC v sestupném směru.

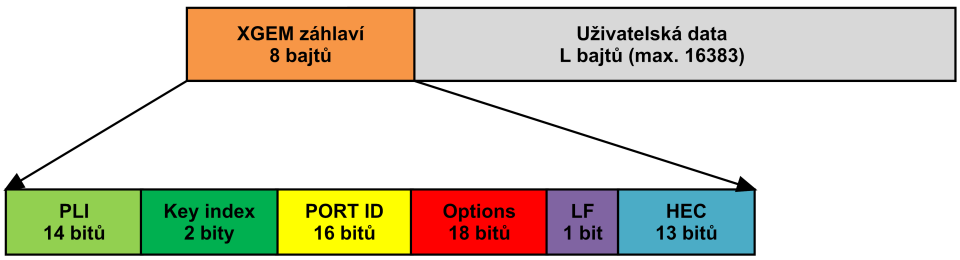
U rámců ve vzestupném směru došlo rovněž k malým úpravám. Pole PLOu obsahuje preambuli sloužící k synchronizaci jednotek OLT a ONU, delimiter označující začátek přenosu ve vzestupném směru, pole ONU-ID s identifikátorem jednotky ONU, indikační pole IND poskytující informace o počtu uživatelských dat čekajících na odeslání a jejich prioritě a pole HEC k detekci a korekci chyb v záhlaví rámce. Další změnou prošlo pole bitové parity BIP, které na rozdíl od rámců GTC už není součástí pole PLOu, ale je umístěno samostatně na konci rámce. Pole PLOAMu a DBRu zůstala beze změn a jejich význam je popsán v kapitole 2.3.1 [11].



Obrázek 2.11: Struktura rámce XGTC ve vzestupném směru.

Uživatelská data jsou zapouzdřena do rámce XGEM (XG-PON Encapsulation Method), viz obrázek 2.12. Tento rámec je opět velmi podobný svému předchůdci a skládá se ze záhlaví o pevné velikosti 8 bajtů a uživatelských dat o proměnlivé délce 0–16383 bajtů. Záhlaví je tvořeno těmito částmi [11]:

- **pole PLI (Payload Length Indicator)**, o velikosti 14 bitů, určuje v bajtech velikost přenášených dat následujících za XGEM záhlavím,
- **pole indexu klíče (Key index)**, pokud byla data šifrována, specifikuje podle kterého klíče,
- **pole Port-ID (Port Identificator)**, o velikosti 16 bitů sloužící k přidělení unikátního čísla portu, na který jsou uživatelská data odeslána, respektive ze kterého byla odeslána,
- **pole Options**, o velikosti 18 bitů určené pro budoucí použití. Hodnota pole je vysílačem nastavena na 0x00000 a přijímač toto pole ignoruje,
- **pole LF (Last Fragment)**, indikuje, jestli se jedná o poslední fragment přenášených dat,
- **pole HEC (Header Error Detection and Correction)**, o velikosti 13 bitů sloužící k zabezpečení přenosu XGEM záhlaví. Poskytuje detekci a opravu chyb. K tomuto účelu je použito kódování BHC (63, 12, 2) v kombinaci s bitovou paritou.



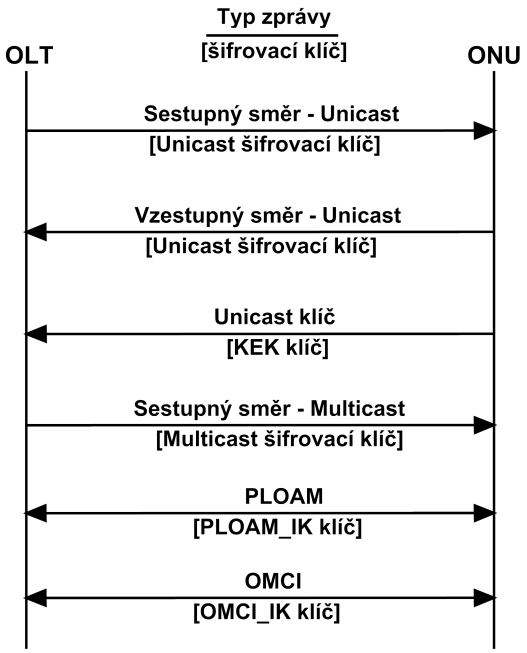
Obrázek 2.12: Struktura rámce XGEM.

2.4.2 Zabezpečení XG-PON

V otázce zabezpečení došlo u systémů XG-PON k poměrně velkým změnám. Novinkou je implementace systému bezpečné výměny šifrovacích klíčů, zabezpečující přenos informací i ve vzestupném směru a implementace oboustranné autentizace centrální OLT

a koncových jednotek. Pro detekci a opravu chyb FEC je v sestupném směru povinná implementace kódu RS(248,216). Ve vzestupném směru je implementace kódování FEC volitelná a je možné použít kód RS(248,232).

Jednotlivé bezpečnostní mechanismy systémů XG-PON jsou v doporučení ITU-T G.987 popsány v různých částech dokumentu a v odlišných kontextech, což může být matoucí. Obrázek 2.13 přehledně ukazuje, které zprávy jsou šifrovány a jakým klíčem [11], [12]:



Obrázek 2.13: Bezpečnostní model XG-PON.

- zprávy zasílané jedinému cíli, neboli unicast, jsou v sestupném směru šifrovány klíčem unicast, který stejně jako v případě systémů GPON vygeneruje jednotka ONU na žádost jednotky OLT,
- unicast zprávy ve vzestupném směru mohou být rovněž zabezpečeny šifrovacím klíčem unicast. Klíč se používá stejný jako ve směru sestupném,
- když dojde k vytvoření nového šifrovacího klíče unicast nebo k jeho úpravě, je tento klíč přenesen k jednotce OLT pod ochranou klíče KEK (Key Encryption Key),
- zprávy zasílané většímu počtu koncových jednotek, neboli multicast, mohou být v XG-PON systémech rovněž šifrovány. Šifrovací klíč multicast vygeneruje jednotka OLT a pošle ho zainteresovaným koncovým jednotkám ONU, ONT prostřednictvím zpráv OMCI pod ochranou klíče KEK,

- zprávy PLOAM a OMCI jsou sice v obou směrech přenášeny nešifrovaně, došlo ale k implementaci zabezpečení integrity pomocí kontroly MIC (Message Integrity Check). MIC mechanismus generuje klíče PLOAM_IK (PLOAM Integrity Key) a OMCI_IK (OMCI Integrity Key), které se používají ke generování a ověřování integrity PLOAM respektive OMCI zpráv.

2.4.3 Derivace bezpečnostních klíčů

Je zjevné, že bezpečnost architektury XG-PON je založena na velkém množství klíčů. Klíče použité pro výměnu zpráv uvedených výše jsou závislé na dalších dvou klíčích, MSK (Master Session Key) a SK (Session Key). Aby celý tento bezpečnostní model měl smysl, je potřeba zajistit bezpečné odvozování jednotlivých klíčů a jejich výměnu.

Proces derivace neboli odvozování klíčů je zachycen na obrázku 2.14. Začíná se klíčem MSK. Tento 128 bitový klíč je výsledkem autentizační procedury a slouží jako startovní bod pro odvozování dalších bezpečnostních klíčů. MSK klíč je vytvořen pomocí algoritmu CMAC (Cipher based Message Authentication Code) v kombinaci se šifrou AES.

Algoritmus CMAC je definován standardem NIST SP800-38B. Obecný zápis tohoto algoritmu je

$$T = AES - CMAC(K, M, Tlen) \tag{2.1}$$

kde T je označení pro výsledný kód, K značí klíč, na který se algoritmus aplikuje, M operand a $Tlen$ velikost výsledného kódu T v bitech.

Pro odvození klíče MSK platí

$$MSK = AES - CMAC((0x55)_{16}, Registration\_ID, 128) \tag{2.2}$$

kde $(0x55)_{16}$ je implicitní klíč v hexadecimálním formátu 0x55 opakovaný 16 krát a Registration_ID je 288 bitová hodnota, která byla přenesena v registrační zprávě PLOAM při připojení koncové jednotky do sítě. Registrační zpráva PLOAM může nabývat konkrétní hodnoty Registration_ID přidělené operátorem sítě nebo implicitní hodnoty $0x00_{36}$.

Klíč SK je odvozen podobným způsobem. Opět je použit algoritmus CMAC, ale s jinými vstupy

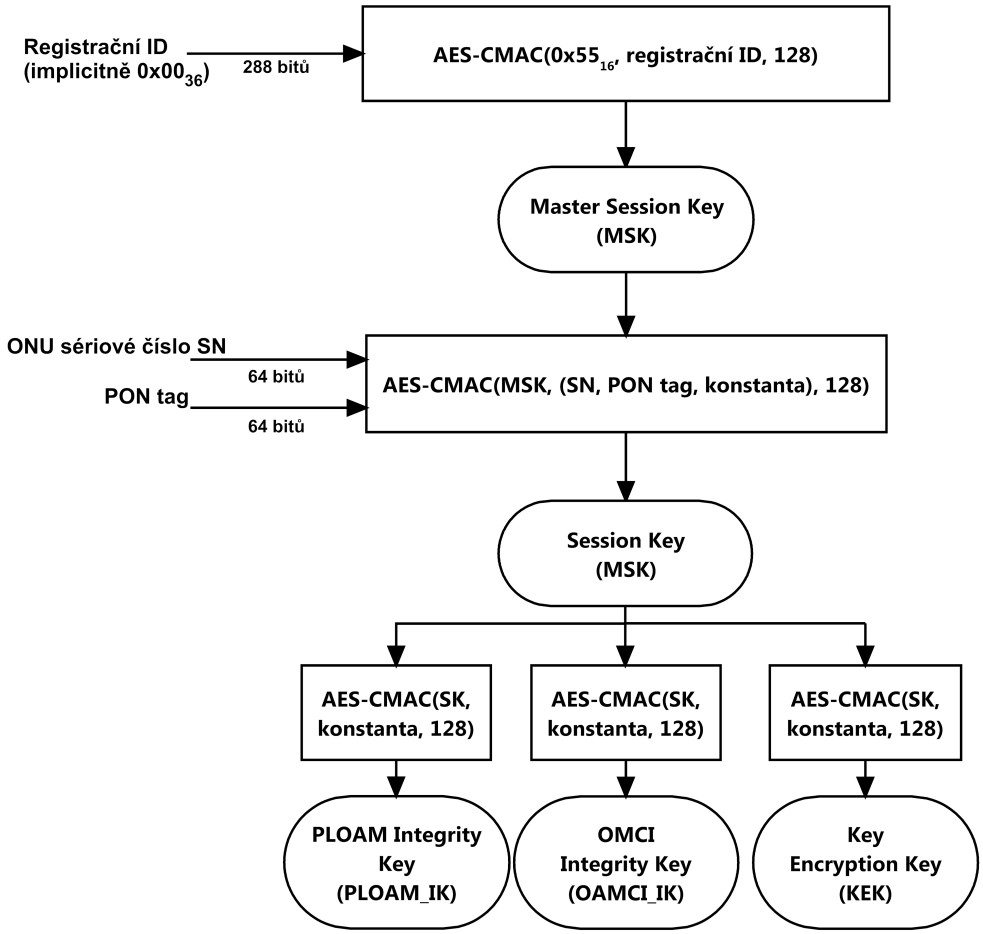
$$SK = AES - CMAC(MSK, (SN, PONtag, konstanta), 128) \tag{2.3}$$

operand v tomto případě tvoří sériové číslo koncové jednotky SN (Serial Number), PON tag označující 8 bajtovou posloupnost definovanou správcem sítě a jako konstanta je použita hodnota 0x53657373696f6e4b, která v ASCII tabulce reprezentuje řetězec „SessionK“.

Pro všechny klíče, které jsou dále odvozené z klíče SK platí

$$Key = AES - CMAC(SK, konstanta, 128) \tag{2.4}$$

odvozované klíče se tedy liší pouze v konstantě. Konstanta klíče PLOAM_IK nabývá hodnoty 0x504c4f414d496e7465677274794b6579 (v ASCII „PLOAMIntegrityKey“), klíč OMCI_IK hodnoty 0x4f4d4349496e746567726974794b6579 (v ASCII „OMCIIntegrityKey“) a klíč KEK hodnoty 0x4b6579456e6372797074696f6e4b6579 (v ASCII „KeyEncryptionKey“) [11], [12].



Obrázek 2.14: Derivace bezpečnostních klíčů v XG-PON.

2.5 EPON (IEEE 802.3ah)

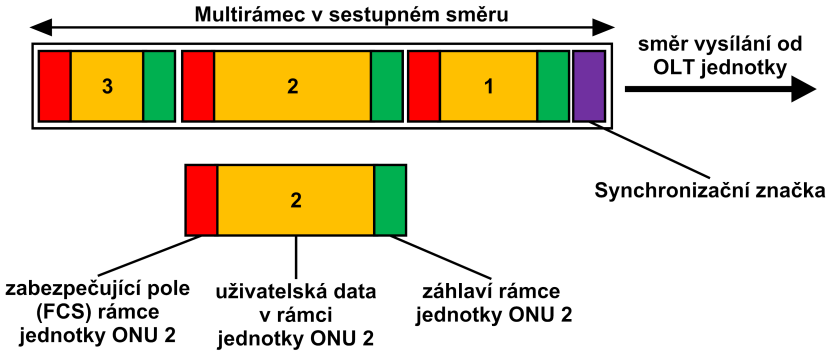
Práci na standardizaci technologie EPON započala v roce 2001 vývojářská skupina pod označením IEEE 802.3ah. Můžeme se setkat i s označením EFM (Ethernet in the First

Mile) neboli Ethernet v první míli. Tato skupina měla za úkol navrhnout koncept a standard pro vysokorychlostní přístupové sítě založené na Ethernetu. Standard byl vydán v roce 2004 a jeho součástí byly i varianty optické přístupové sítě EPON 1000BASE-PX10 a 1000BASE-PX20 označované též EPON typ 1 a typ 2.

EPON typ 1 umožňuje při použití jednoho jednovidového vlákna připojit maximálně 16 uživatelů a dosáhnout vzdálenosti pouze 10 km. Protože EPON typ 2 umožňuje připojit až 32 uživatelů a maximální dosah této varianty je 20 km tak se v praxi EPON typ 1 téměř nepoužívá. Přenosová rychlost obou variant EPON byla stanovena 1,25 Gbit/s symetricky. Obousměrný provoz je řešen stejně jako u technologií v rámci doporučení ITU-T a v každém směru je pro přenos použita jiná vlnová délka. Ve směru sestupném je použita vlnová délka z pásma 1480–1500 nm a ve směru vzestupném z pásma 1260–1360 nm [13].

2.5.1 Přenos v EPON

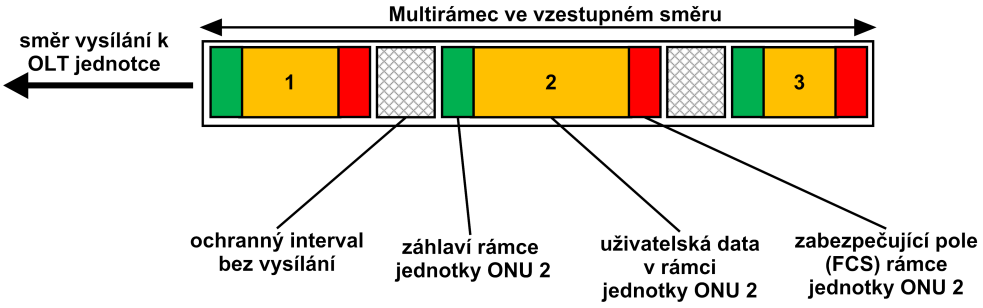
Schéma přenosu je shodné s ostatními technologiemi postavených na časovém dělení. V sestupném směru jsou z jednotky OLT kontinuálně vysílány časové multirámce, ve kterých jsou pomocí časového multiplexu umístěna data jednotlivých koncových jednotek. Na rozbočovačích jsou tyto multirámce všesměrově přeposlány na koncové jednotky, které si podle identifikátoru vyberou jim určenou část a zbytek zahodí. Datové jednotky jsou v multirámci uloženy ve formě Ethernet rámců s kódováním 8B/10B a navzájem odděleny záhlavím rámce z jedné strany a zabezpečovacím polem rámce ze strany druhé. Začátek multirámce je označen synchronizační značkou. Strukturu multirámců zachycují obrázky 2.15 a 2.16.



Obrázek 2.15: Struktura multirámce architektury EPON v sestupném směru.

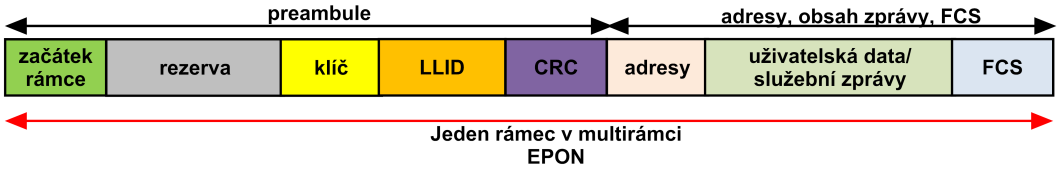
Ve vzestupném směru mají koncové jednotky přidělené časové intervaly, tzv. time sloty ve kterých mohou vysílat. V jednom time slotu může jednotka přenášet několik

Ethernet rámců. Koncové jednotky jsou synchronizovány, aby při přenosu nedošlo ke kolizím. Z tohoto důvodu jsou navíc jednotlivé rámce v multirámci odděleny ochranným intervalem, během něhož se nevysílá.



Obrázek 2.16: Struktura multirámce architektury EPON ve vzestupném směru.

Každý Ethernetový rámec je tvořen dvěma částmi. První část, záhlaví (preambule) se skládá z pole vymezujícího začátek rámce (1 bajt), identifikátoru LLID (Logical Link ID – 2 bajty), šifrovacího klíče (1 bajt) a pole CRC (1 bajt) pro zabezpečení preambule. Zbývající 3 bajty jsou rezervní. Druhá část obsahuje uživatelská data, zdrojovou a cílovou MAC adresu, služební zprávy o velikosti a typu přenášeného obsahu a pole FCS (Frame Check Sequence) k detekci případných chyb vzniklých při přenosu rámce [13]. Struktura Ethernet rámce je zobrazena na obrázku 2.17.



Obrázek 2.17: Struktura rámce Ethernet v architektuře EPON.

2.5.2 Zabezpečení EPON

Standard IEEE 802.ah nespecifikuje bezpečnostní a ochranné mechanismy pro systémy EPON. Případná implementace bezpečnostních mechanismů je plně v kompetenci jednotlivých výrobců daných optických jednotek, kteří tyto mechanismy implementují s ohledem na konkrétní požadavky zákazníka. Typicky bývá implementováno šifrování metodou AES a některý z modelů autentizace. Podobně je nahlíženo i na implementaci opravného kódování FEC v podobě kódu RS(255,239), které je sice standardem doporučeno, avšak není striktně vyžadováno [14].

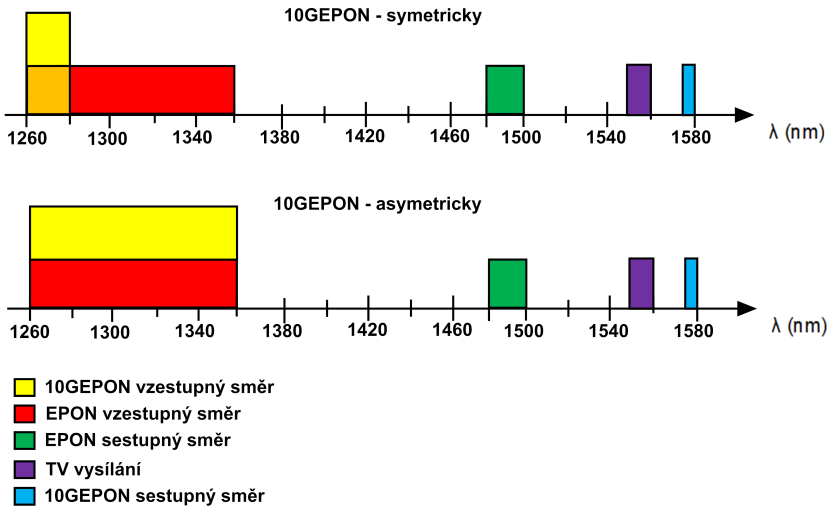
2.6 10GEPON (IEEE 802.3av)

I technologie EPON se dočkala svého deseti gigabitového následovníka. V roce 2006 byl v rámci standardu IEEE 802.3av zahájen vývoj technologie s označením 10GEPON. Tento standard byl dokončen v roce 2009.

Stejně jako u EPON je klíčovým protokolem druhé vrstvy Ethernetový rámec. K velkým změnám však došlo u některých parametrů sítě. Kromě navýšení přenosových rychlostí byly zavedeny nové útlumové třídy, pro kompatibilitu se systémy EPON bylo potřeba přizpůsobit použité vlnové délky a došlo k zavedení nového překódování Ethernet rámců 64B/66B, které výrazně snižuje režii kódu.

U systémů 10GEPON máme na výběr symetrický i asymetrický režim rychlostí. Symetrický režim nabízí rychlost 10 Gbit/s v obou směrech, v asymetrickém režimu je rychlost v sestupném směru 10 Gbit/s a ve vzestupném směru 1 Gbit/s. Asymetrický režim byl zaveden především s ohledem na nižší nákladovost. Využívá se zde jiné vlnové pásmo, které umožňuje použití levnějších optických zdrojů v koncových jednotkách, navíc je rychlost 1 Gbit/s v mnoha síťových zapojeních stále dostatečná.

Pro symetrický režim jsou představeny nové útlumové třídy PR10, PR20, PR30 a pro asymetrický režim PRX10, PRX20, PRX30. Útlumová třída určuje minimální dosah a dělící poměr. PR10 a PRX10 určuje minimální dělící poměr 1:16 s dosahem alespoň 10 km. PR20 a PRX20 minimální poměr 1:16 a dosah 20 km nebo poměr 1:32 s dosahem 10 km. PR30 a PRX30 určuje minimální poměr 1:32 s dosahem alespoň 20 km. Vyšší počet útlumových tříd umožní provozovateli zvolit optimální variantu a zvýšit tak úsporu nákladů.



Obrázek 2.18: Pásma vlnových délek pro EPON, 10GEPON a služby TV vysílání.

Pro zachování kompatibility s EPON byla pro sestupný směr zvolena vlnová délka z pásma 1575–1580 nm a ve vzestupném směru je vlnová délka odlišná pro symetrický a asymetrický režim. Pro symetrický režim je použita délka z pásma 1260–1280 nm a pro asymetrický režim z pásma 1260–1360 nm. Použitá vlnová pásma jsou zachycena na obrázku 2.18. K oddělení optických signálů systémů EPON a 10GEPON, jejichž vlnová pásma se ve vzestupném směru překrývají, je použit časový multiplex TDM [15].

2.6.1 Zabezpečení 10GEPON

Stejně jako v případě EPON se standard architektury 10GEPON otázkou bezpečnosti nezabývá. Implementace mechanismů pro ochranu sítě a přenosu informací je v kompetenci jednotlivých výrobců. Drobnou změnou je nyní povinná implementace FEC kódu RS(255,223) [15].

2.7 Porovnání technologií TDM-PON

V tabulce 2.3 jsou zachyceny parametry všech technologií TDM-PON. Základním měřítkem porovnání je použitý protokol 2. vrstvy a přenosová rychlost. Technologie nejsou vzájemně kompatibilní, vyjímkou je kompatibilita technologie GPON s XG-PON a EPON s 10GEPON. Míra zabezpečení se nedá u technologií EPON a 10GEPON objektivně posoudit, neboť jejich bezpečnostní mechanismy nejsou pevně dány.

Tabulka 2.3: Porovnání technologií TDM-PON.

Technologie	APON/BPON	GPON	XG-PON	EPON	10GEPON
Doporučení	ITU-T G.983	ITU-T G.984	ITU-T G.987	IEEE 802.3ah	IEEE 802.3av
Vlnová délka - sestupný směr	~1490 nm	~1490 nm	~1580 nm	~1490 nm	~1580 nm
Vlnová délka - vzestupný směr	~1310 nm	~1310 nm	~1270 nm	~1310 nm	~1310 nm
Přenosová rychlost	Až 1244,16 Mbit/s	Až 2488,32 Mbit/s	10 Gbit/s	1,25 Gbit/s	10 Gbit/s
Max. rozbočovací poměr	1:16	1:64	1:256	Typ 1 - 1:16 Typ 2 - 1:32	1:128
Protokol 2. vrstvy	ATM	GEM	xGEM	Ethernet	Ethernet
Dosah	20 km	20 km	20 km	10/20 km	10/20 km
Míra zabezpečení	Nízká	Střední	Vysoká	-	-

3 Technologie WDM-PON

Tradiční systémy PON založené na časovém dělení TDM se pomalu blíží k hranici, kdy jejich parametry přestanou být dostatečné pro stále zvyšující se požadavky provozovatelů optických sítí. Budoucností jsou pasivní optické sítě založené na vlnovém dělení WDM.

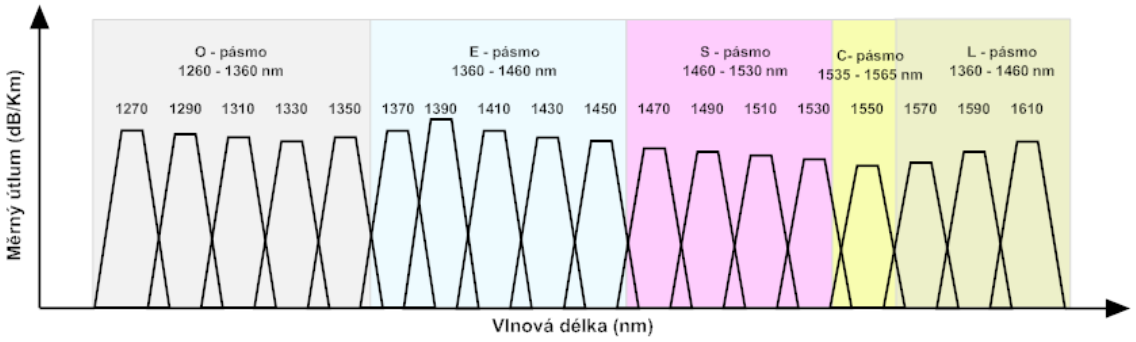
Technologie vlnového dělení WDM umožňuje paralelně přenášet po jednom optickém vlákně několik navzájem oddělených vlnových délek. Velká výhoda oproti TDM-PON spočívá v přidělení vlastní vlnové délky každému účastníkovi, který tak má přístup k celé šířce pásma. Nejen že se takto zvyšuje celková kapacita sítě, ale dochází i ke zvýšení bezpečnosti sítě. Z pohledu fyzické vrstvy se mezi jednotkami OLT a ONU vytvoří spojení typu bod - bod a je tak znemožněn odposlech přenášených dat. Dochází i k zjednodušení přenosu na druhé vrstvě modelu, jelikož odpadá potřeba implementace podvrstvy pro ovládání vícenásobného přístupu k médiu MPCP (MultiPoint Control Protocol). Další nespornou výhodou je flexibilita sítě, která umožňuje jednotlivým koncovým jednotkám pracovat s různými přenosovými rychlostmi a protokoly podle aktuálních požadavků.

Nevýhodou ve srovnání se systémy TDM-PON je především vysoká pořizovací cena. Je zapotřebí složitější jednotka OLT, která umí vysílat na více vlnových délkách a laditelný laser v koncových jednotkách, který umožní uživateli naladit jemu přidělenou vlnovou délku.

Technologie sama o sobě zatím není standardizována, ale díky doporučení ITU-T G.694 došlo alespoň k jednotnému určení vlnových délek pro realizaci vlnového dělení a došlo k rozdělení na variantu hrubého CWDM (Coarse WDM) a hustého DWDM (Dense WDM) vlnového dělení podle vzájemného odstupu vlnových délek [6].

3.1 CWDM

Představuje ekonomičtější variantu vlnového dělení. Doporučení ITU-T G.694.2 definuje 18 kanálů s roztečí 20 nm (2500 GHz) a tolerancí na každém kanálu 6,5 nm, ve vlnovém pásmu od 1260–1620 nm. Větší rozteč kanálů a dodatečná tolerance umožňuje použití méně kvalitních a teplotně nestabilizovaných optických zdrojů. Systémy CWDM se nejvíc využívají v metropolitních sítích a umožňují na každém kanále přenos Gbit Ethernet do vzdálenosti 80 km a rychlosti 2,5 Gbit/s do vzdálenosti 50km. Nevýhodou je menší počet kanálů ve srovnání s DWDM [16].



Obrázek 3.1: Kanály CWDM definované v ITU-T G.694.2.

3.2 DWDM

Tento systém vydělování vlnových délek se řadí mezi nejdokonalejší systémy používané v optoelektronice. Princip je založen na velmi malých vzdálenostech mezi jednotlivými kanály. Doporučení ITU-T G.694.1 specifikuje přenosové kanály z oblasti vlnových délek 1490–1620 nm, představující tzv. S (Short), C(Conventional), L (Long) pásmo. Běžná rozteč mezi jednotlivými kanály je 0,8 nm (100GHz) a 0,4 nm (50GHz). Některé technologie jsou schopné pracovat s rozestupy až 0,1 nm (12,5 Ghz), jedná se o tzv. ultra DWDM. V daném vlnovém rozsahu tyto rozestupy představují desítky přenosových kanálů.

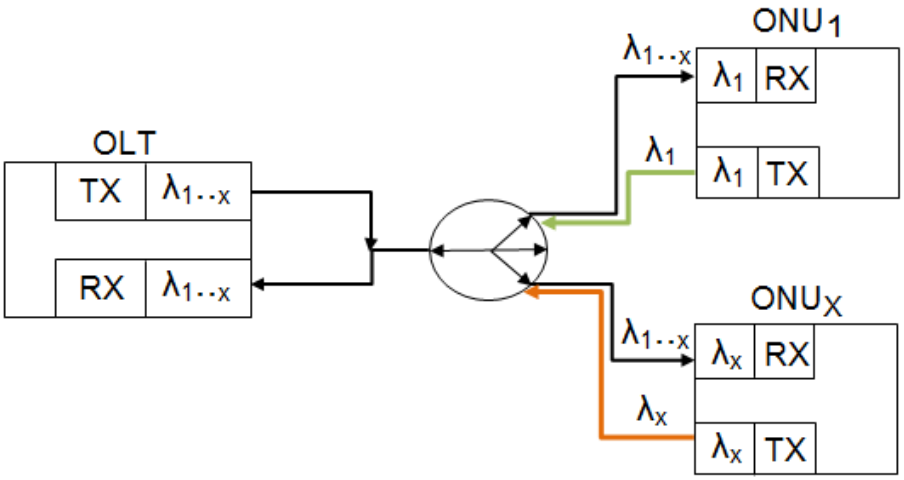
Dnešní DWDM systémy umožňují na jednom fyzickém spoji přenos až 96 kanálů s přenosovou rychlostí 2,5–10 Gbit/s na každém kanálu. Nevýhodou těchto systémů je nutnost použití vysoce stabilních optických zdrojů (chlazené lasery) a přesných optických filtrů, které jsou cenově velmi nákladné [16].

3.3 Varianty WDM-PON

V závislosti na použitých prvcích a typu realizace se můžeme setkat se čtyřmi variantami systémů WDM-PON.

První varianta, viz obrázek 3.2, počítá s pevně přidělenými vlnovými délkami každé z koncových jednotek. V síti je použit klasický rozbočovač, tzn. že v sestupném směru je signál z jednotky OLT všesměrově rozeslán na všechny koncové jednotky. Koncové jednotky obdrží signál na všech vlnových délkách a pomocí pevně nastaveného vlnového filtru oddělí část určenou pro svou vlnovou délku. Ve vzestupném směru má každá jednotka individuální vlnovou délku, na které vysílá odchozí data. Jedna vlnová délka je společná pro všechny koncové jednotky a slouží pro přenos broadcast zpráv. Výhodou použití pasivního rozbočovače je jeho jednoduchost a cena. Distribuční síť je zachována,

stačí pouze vyměnit hardwarové prvky. Nevýhodou je vysoký vložný útlum limitující počet připojených jednotek a bezpečnostní riziko spojené s šířením signálu na všechny koncové jednotky, vyžadující implementaci mechanismů proti odposlechu. Kvůli pevně přiděleným vlnovým délkám je další nevýhodou nepružnost sítě a nehospodárné nakládání s přenosovými kapacitami. V těchto sítích rovněž nemůžou existovat dvě jednotky komunikující na stejné vlnové délce [17].



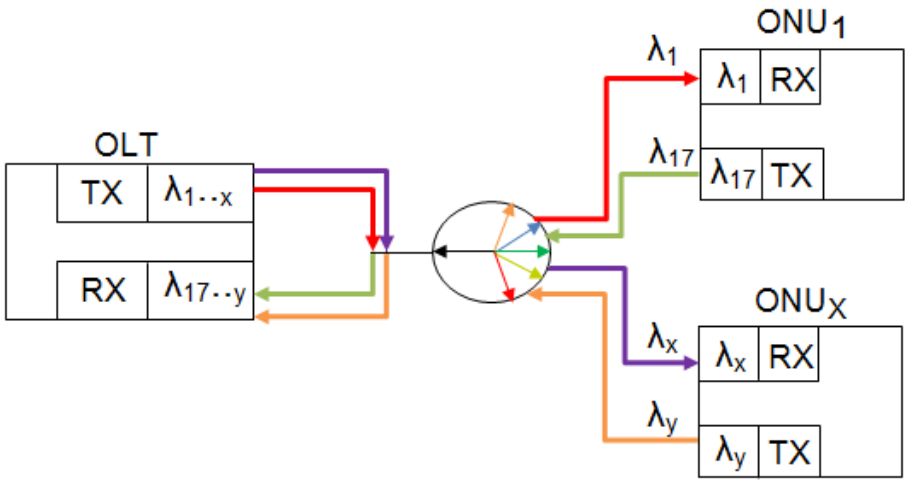
Obrázek 3.2: WDM-PON s pevně přidělenými vlnovými délkami.

Ve druhé variantě je místo klasického rozbočovače použita směrová odbočnice AWG (Arrayed Waveguide Grating), viz obrázek 3.3. V sestupném směru je signál přicházející z jednotky OLT pomocí AWG vydělen na jednotlivé vlnové délky, které se ke koncovým jednotkám šíří v separátních kanálech. Princip přenosu ve vzestupném směru je stejný jako při použití rozbočovače, každá jednotka vysílá na své vlnové délce. Výhodou použití AWG je snížení vložného útlumu, typicky kolem 5 dB. Další výhodou je odstranění vstupních WDM filtrů z koncových jednotek, což rovněž vede ke snížení celkového útlumu [17].

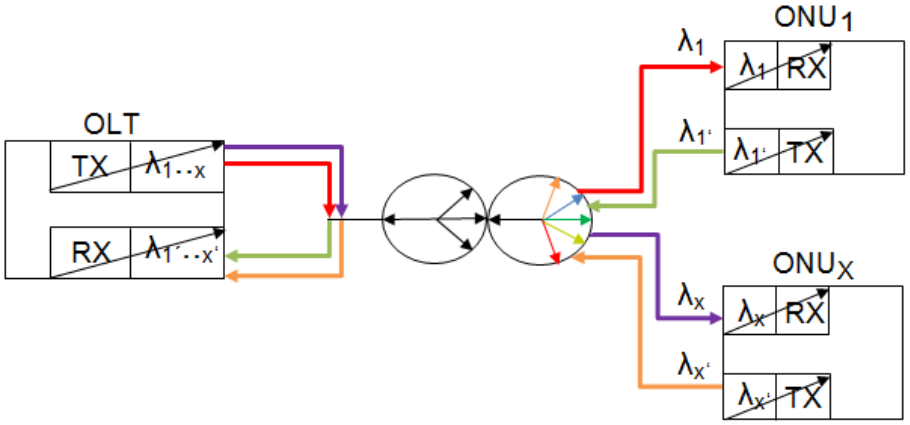
Třetí varianta je založena na kombinaci rozbočovače a odbočnic AWG. Na jednotlivé výstupy rozbočovače je připojena odbočnice AWG nebo více odbočnic v kaskádě, viz obrázek 3.4. Tímto dosáhneme přesnějšího vydělování vlnových délek, což je předpoklad pro nasazení metody DWDM. Použití univerzálních koncových jednotek a volitelných vlnových délek umožňuje přidělovat kanály jednotkám podle aktuální potřeby a požadavků. Tento proces se označuje jako DWA (Dynamic Wavelength Assignment).

Ve vzestupném směru se předpokládá použití širokopásmového optického zdroje s využitím metody spectrum-slicing nebo sdílený kanál s použitím metody TDMA označovaný jako CPON (Composite PON). Nevýhodou tohoto zapojení je vysoká cena po-

užitých komponent. Je potřeba implantovat aktivní přeladitelné optické filtry a zdroje do všech jednotek [17].



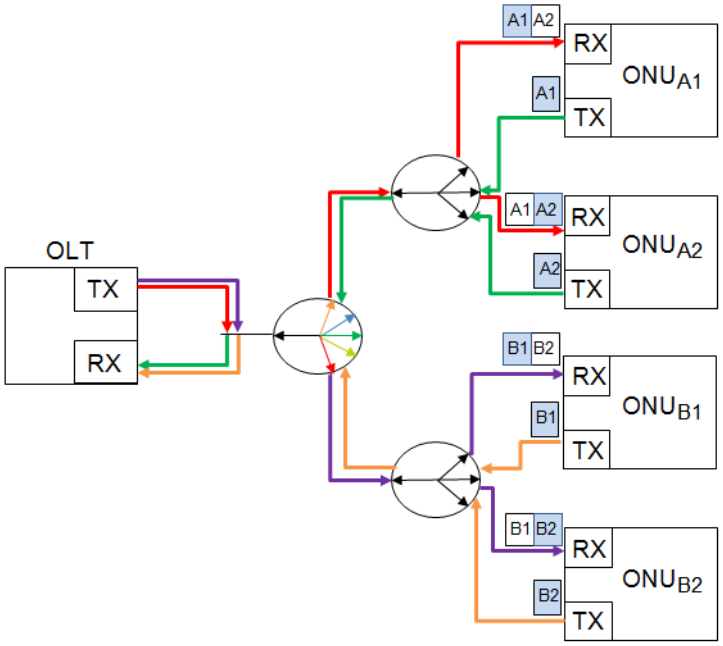
Obrázek 3.3: WDM-PON s vydělováním délek pomocí odbočnice AWG.



Obrázek 3.4: WDM-PON s kaskádním zapojením rozbočovače a odbočnic AWG.

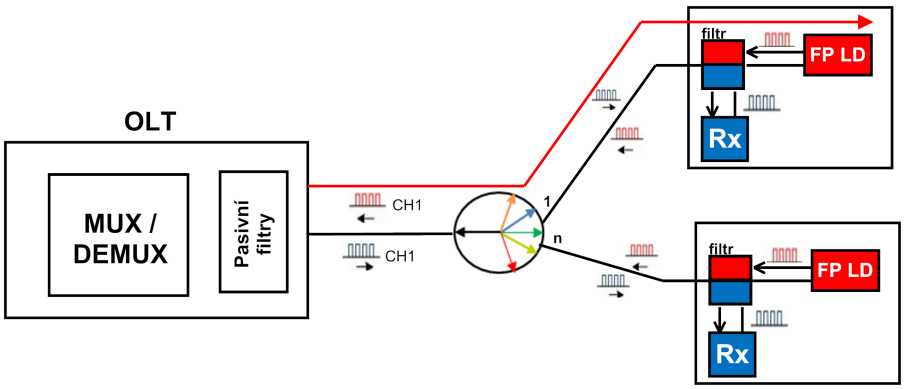
Poslední varianta se označuje jako hybridní WDM-PON nebo také WDM/TDM-PON. Tento typ realizace nabízí nejefektivnější využití přenosových prostředků s maximálním počtem připojených uživatelů. Princip spočívá v zapojení jednoho typu WDM-PON a připojení technologie EPON/GPON na jednotlivé kanály. Na těchto kanálech pak budou přenášena data pro větší počet koncových jednotek, viz obrázek 3.5. Pokud by například byla použita technologie DWDM s 32 kanály, tedy 64 vlnovými délkami a technologie GPON s maximálním počtem 32 připojených jednotek, může tato síť obsloužit 32x32 = 1024 uživatelů. Aby bylo dosaženo maximální efektivity, měla by být součástí

těchto systémů implementace dynamického přidělování časových slotů a vlnových délek podle požadavků koncových jednotek, označována DWA/DBA. Toto se ovšem opět odrazí na ceně koncových jednotek, jejichž součástí musí být přeladitelné optické zdroje [1].



Obrázek 3.5: Hybridní WDM/TDM-PON.

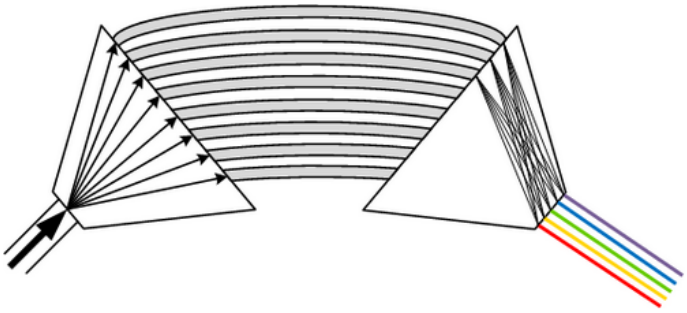
V praktické části této práce je použita varianta WDM-PON s odbočnicí AWG, kde jsou jako zdroje optického signálu v jednotkách ONU použity lasery FP (Fabry–Pérot), viz obrázek 3.6. V koncových jednotkách osazených tímto typem laserů se nachází filtr, který rozdělí přicházející paprsek širokopásmového světelného zdroje BLS (Broad-band Light Source) z jednotky OLT do dvou úseků. Signál pro příchozí směr je na filtru oddělen a pokračuje do přijímací části jednotky ONU. Druhá část signálu projde skrze filtr a pokračuje na FP laser. Zde dojde k zavěšení laseru FP na stimulační vlnovou délku, což vede ke změně spektra, původně tvořeného periodickými vlnami na spektrum s úzkou spektrální čarou. Tím je umožněno použít laser FP jako vysílač pro systém WDM-PON [16].



Obrázek 3.6: WDM-PON s využitím laserů Fabry-Perot.

3.4 Princip AWG

Na vstupu odbočnice AWG je optický paprsek přiveden do širšího vlnovodu, ze kterého se po krátké vzdálenosti rozdělí do většího počtu užších vlnovodů. Tyto menší vlnovody jsou stáčeny tak, že vytváří téměř soustředěné kruhové výseče o různé délce. Konec vlnovodů je opět vyveden na širší vlnovod, zakončený jednotlivými výstupy s již vydělenými vlnovými délkami. Využívá se zde fázového posuvu jednotlivých vlnových délek, vznikajícího průchodem úzkými vlnovody s rozdílnou délkou. Princip tohoto vydělování je zobrazen na obrázku 3.7. [17]



Obrázek 3.7: Princip vydělování vlnových délek odbočnicí AWG. [17]

4 Bezpečnost sítě

Systémy PON, stejně jako každý jiný typ komunikační sítě, ve kterém jsou přenášeny důvěrné a citlivé informace, by měly dodržovat určitá bezpečnostní pravidla. Standard ISO 7498-2 ISO/OSI Security Architecture definuje základní bezpečnostní funkce pro komunikační sítě, které mohou být implementovány na různých vrstvách modelu a rozděluje je do pěti skupin [18]:

- **služby autentizace** – jedná se o ověření identity jedné nebo obou stran komunikace,
- **služby řízení přístupu (autorizace)** – ochrana před neautorizovaným využíváním služeb a přístupu k síťovým prostředkům,
- **služby zajištění důvěrnosti** – ochrana přenášených informací před neautorizovaným odhalením,
- **služby zajištění integrity** – ochrana před neautorizovanou modifikací přenášených informací,
- **služby pro nepopíratelnost** – ochrana znemožňující odesílateli respektive příjemci popřít odeslání a přijmutí zprávy.

Z uvedeného výčtu bezpečnostních funkcí, které by měly komunikační sítě poskytovat je v optických přístupových sítích nejvyšší důraz kladen na zajištění důvěrnosti a ověření identity. Implementace ostatních služeb buď to chybí anebo je řešena až na vyšších vrstvách modelu [19].

4.1 Bezpečnostní rizika systémů TDM-PON

V systémech TDM-PON pochází většina bezpečnostních rizik ze samotného principu přenosu, kde koncové jednotky ONU sdílí společné médium a signál v sestupném směru je šířen od jednotky OLT k těmto jednotkám všesměrově.

S přenosem dat v systémech TDM-PON jsou spojena bezpečnostní rizika odposlechu dat, krádeže identity a odepření služby DoS (Denial Of Service) [14].

4.1.1 Odposlech služebních zpráv

V systémech APON, EPON, 10GEPON a GPON mohou být v sestupném směru zabezpečena pouze uživatelská data. Záhlaví datových jednotek s obsahem služebních a řídících zpráv, adresy a identifikátory jednotlivých koncových jednotek jsou přenášeny nezabezpečeně.

Protože jsou jednotky ONU umístěny u koncových uživatelů, nemusí být fyzický přístup k nim složitý. Potencionálnímu útočníkovi poté stačí přeprogramovat jednotku do tzv. promiskuitního režimu, kdy úpravou programového vybavení dojde k vyřazení hardwarového filtru a jednotka může bez problémů odchytávat všechna data posílaná v sestupném směru. Útočník takto získá přístup k nezabezpečeným informacím o počtu aktivních koncových jednotek, přiřazené vysílací kapacitě těmto jednotkám a další informace, týkající se aktuálního provozu v síti.

Nebezpečí odposlechu je o to větší, že upravená jednotka ONU se navenek chová normálně a odposlech probíhá pasivně. Detekce tohoto typu útoku je proto velmi obtížná [14].

4.1.2 Odposlech ve vzestupném směru

V systémech TDM-PON dlouho panoval předpoklad, že vzhledem k směrově orientovaným vlastnostem přenosu by koncová jednotka neměla být schopna přijímat data vysílaná z jiných koncových jednotek. Proto jsou veškeré informace, včetně bezpečnostních klíčů, ve vzestupném směru posílány nezabezpečeně. Ukázalo se ale, že tento předpoklad je mylný.

Na popud praktických zkušeností operátorů provozujících systémy PON a následně provedených testech a měření bylo zjištěno, že za určitých podmínek (nečistoty konektorů, použitá topologie, kvalita optických vláken) je v některých případech možné probíhající komunikaci ve vzestupném směru zachytávat a odposlouchávat a to díky odrazům signálu, které mohou kvůli výše zmíněným podmínkám vzniknout. Případné odrazy se od místa odrazu šíří sestupným směrem a díky rozbočovačům jsou doručeny až k jednotlivým koncovým jednotkám. Provoz v sestupném směru není těmito odrazy rušen, protože probíhá v jiném vlnovém pásmu. Z tohoto důvody není možné pro zachycení odrazů použít obyčejnou jednotku ONU, ale je potřeba speciální detektor schopný přijímat data na vlnové délce vzestupného směru. Řešením tohoto typu odposlechu je implementace šifrování ve vzestupném směru, k čemuž již došlo u technologie XG-PON [14].

4.1.3 Odposlech v sestupném směru

Uživatelská data v sestupném směru jsou šifrována v případě technologie GPON, XG-PON mechanismem AES viz kapitola 4.3.2. Pro technologie EPON, 10GEPON není metoda šifrování striktně dána a využívá se proprietárních řešení jednotlivých výrobců těchto systémů, obvykle bývá implementována metoda AES. Hrozbu odposlechu ko-

munikace v sestupném směru představuje především riziko odposlechu vzestupného směru a s tím spojené odcizení šifrovacího klíče. Pokud by se útočníkovi podařilo z provozu vzestupného směru získat šifrovací klíč a poté přeprogramovat koncovou jednotku do promiskuitního režimu, může všechna přenášená data kompromitovaného uživatele bez problémů dešifrovat do původní podoby [14].

4.1.4 Impersonace

Protože bývají nezabezpečeně přenášeny rovněž unikátní, identifikační značky koncových jednotek, reálně hrozí jejich odcizení a zneužití. Na základě odcizeného identifikátoru se může útočník vydávat za jinou koncovou jednotku v téže síti a mít tak přístup k informacím a službám kompromitovaného uživatele. Pro zabránění odcizení a zneužití identifikátoru je potřeba implementovat zabezpečení přenášených služebních zpráv v kombinaci s autentizací [14].

4.1.5 Odepření služby

Hrozba odepření služby DoS (Denial of Service) je v systémech TDM-PON vysoká. Je to dáno povahou přenosu uskutečněného skrze médium sdílené všemi účastníky. Tímto rizikem sice nejsou bezprostředně ohrožena přenášená data, ale je ohrožena dostupnost určitých služeb, případně celé sítě ostatním uživatelům.

Pokud by koncová jednotka vysílala signál mimo své vyhrazené časové okamžiky, došlo by na rozbočovači ke kolizi časových rámců této jednotky s časovými rámci z ostatních jednotek a tím k jejich znehodnocení. K odepření služby může dojít poruchou na koncové jednotce nebo být záměrně vyvolán útočníkem, který přeprogramuje jednotku, případně připojí jiný optický zdroj, který bude vysílat nepřetržitý optický signál dostatečné úrovně a zablokuje jim část nebo celý provoz ve vzestupném směru. V současných systémech PON chybí mechanismy pro určení původu DoS a řešení tohoto problému často vyžaduje přítomnost technika a následné manuální odpojování jednotlivých jednotek [14].

4.2 Bezpečnostní rizika systémů WDM-PON

Ačkoliv se obecně předpokládá, že systémy WDM-PON poskytují bezpečnější formu přenosu informací, než sítě postavené na některé z technologii TDM-PON, není to vždy pravda. Základním měřítkem, které určuje míru zabezpečení je, která z variant zapojení WDM-PON popsaných v kapitole 3.3 je použita.

Při použití varianty s klasickým rozbočovačem a varianty hybridního zapojení jsou rizika přenosu informací z důvodu všesměrové povahy šíření signálu totožná s riziky

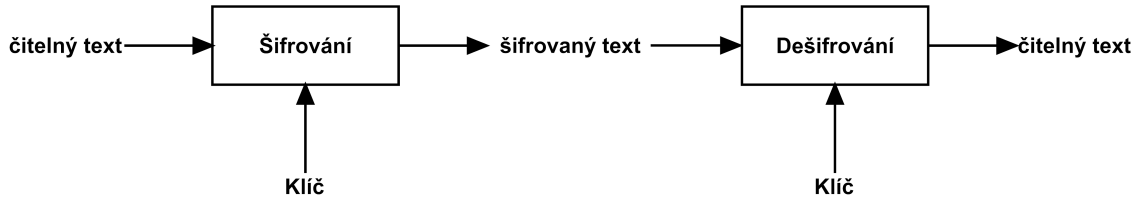
systémů TDM-PON. Z pohledu bezpečnosti u těchto typů zapojení nedochází k žádnému zlepšení a je nutné implementovat mechanismy k zabezpečení přenosu.

Naopak varianta s odbočnicí AWG a případné kaskádní zapojení odbočnic AWG a rozbočovače zvyšuje zabezpečení sítě velmi znatelně. Mezi jednotkou OLT a koncovými jednotkami ONU je z pohledu fyzické vrstvy vytvořeno spojení typu bod–bod a koncové jednotky tak mají přístup k pouze jim určeným informacím. Ze stejného důvodu u těchto variant rovněž odpadá hrozba odepření služby DoS nebo impersonace.

Jedinou hrozbou systémů WDM-PON využívajících k šíření signálu odbočnice AWG, je možnost existence přeslechů mezi jednotlivými kanály. Protože technika vydělování vlnových délek na odbočnicích AWG není dokonale přesná, dochází obvykle k přenosu signálu malé úrovně i z přilehlých dvou kanálů původní vlnové délky. Odfiltrováním těchto přeslechů a jejich následným zesílením je teoreticky možné přijímat data původně určená jiným koncovým jednotkám. Ověření míry nebezpečí této hrozby je náplní praktické části této bakalářské práce, viz kapitola 5 [28].

4.3 Šifrování

K zajištění důvěrnosti, tedy zajištění aby neoprávněný posluchač datům přenášeným na kanále nerozuměl, se používá metoda označována jako kryptografie neboli šifrování. Jedná o algoritmus, který převádí čitelný (prostý) text do nečitelné podoby (šifrovaný text). Toho je dosaženo použitím tajné informace v podobě šifrovacího klíče, viz obrázek 4.1. Podle přenosu klíče se kryptografie rozděluje na symetrickou a asymetrickou [20].



Obrázek 4.1: Obecný algoritmus kryptografie.

4.3.1 Šifra Churning

Tato šifra byla poprvé představena v doporučení ITU-T G.983 a měla poskytnout ochranu přenášených dat před odposlechem.

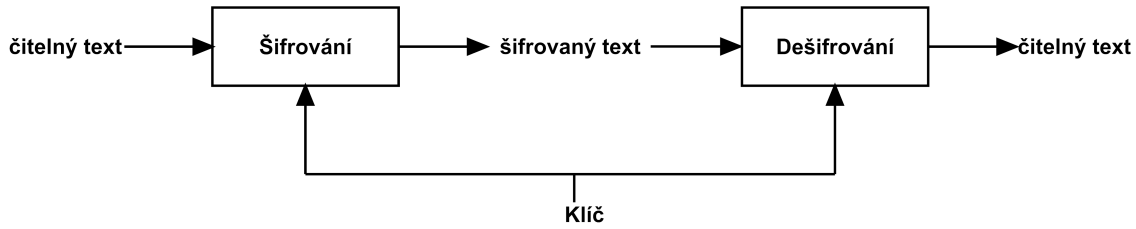
Jedná se o substituční šifru tzn., že podle šifrovacího klíče dochází k záměně množiny bitů za jinou stejně velkou množinu. Konkrétně u této šifry je 8 bitový prostý text podle 24 bitového klíče převeden na 8 bitový zašifrovaný text. Pro větší odolnost je šifrovací

klíč vytvářen XOR funkcí 24 bitové náhodné posloupnosti a 24 bitů náhodných dat extrahovaných z přenosu vzestupného směru. Nový klíč je generován koncovou jednotkou minimálně jednou za vteřinu.

Jelikož se později ukázalo, že je tato metoda šifrování velmi snadno prolomitelná a to hned několika typy útoků, byla do doporučení ITU-T G.983.3 dodatečně přidána podpora AES šifrování s klíčem o délce 128 bitů [8], [29].

4.3.2 Symetrické šifrování

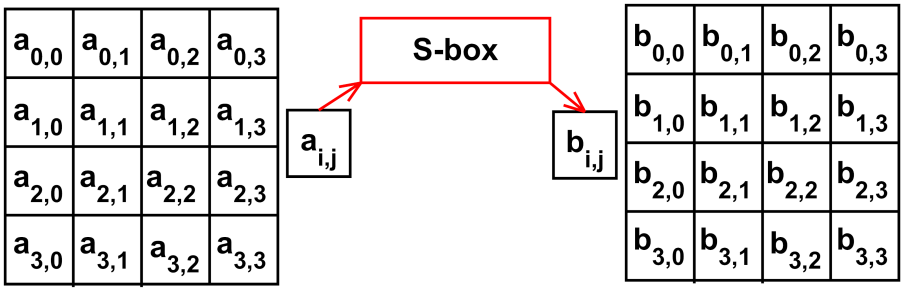
Symetrická kryptografie spočívá ve sdílení šifrovacího klíče. K šifrování a dešifrování je použit tentýž klíč, viz obrázek 4.2. Výhodou těchto algoritmů je jejich jednoduchost a rychlost, lze je implementovat hardwarově i softwarově. Nevýhodou je nutnost zajištění bezpečné výměny šifrovacího klíče. Mezi symetrické šifry patří algoritmy DES, 3DES, AES [21].



Obrázek 4.2: Algoritmus symetrického šifrování.

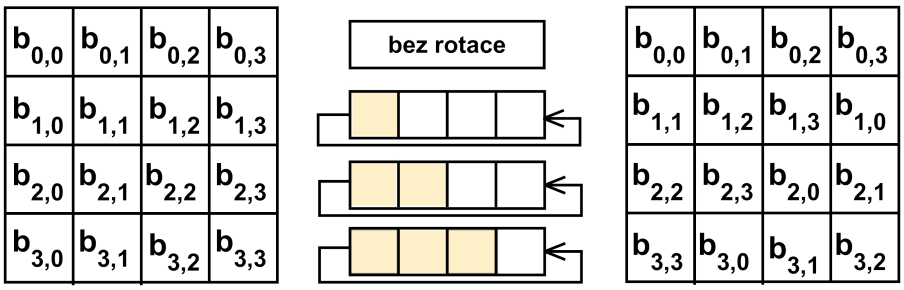
Poslední jmenovaný AES (Advanced Encryption Standard) je nejčastěji využívaným šifrovacím algoritmem v systémech PON a komunikačních sítích obecně, hojně se s ním setkáme například u bezdrátových sítí. Předností tohoto algoritmu je jednoduchá implementace a rychlost šifrování dat (> 360Mbit/s). Jedná se o blokovou šifru pracující s bloky o velikosti 128, 192 nebo 256 bitů. Pokud je velikost přenášených dat větší, rozdělí se do více bloků a případné volné místo v posledním bloku je nahrazeno výplní. Velikost šifrovacího klíče může být opět 128, 192 nebo 256 bitů nezávisle na velikosti bloku. Všechny operace v AES se provádějí na 2-D poli označovaném Stav (State) a celý proces šifrování tvoří 10 až 14 iterací (rund), kde se každá iterace provede ve 4 krocích [22]:

- **SubBytes** – tato operace zajistí nelineárnost šifry a jejím cílem je zabránění útokům založených na jednoduchých algebraických vlastnostech. Jedná se o substituci, kde každý bajt stavové matice je nahrazen jiným bajtem podle předem daného klíče, určeného tabulkou Rijndael-S, viz obrázek 4.3,



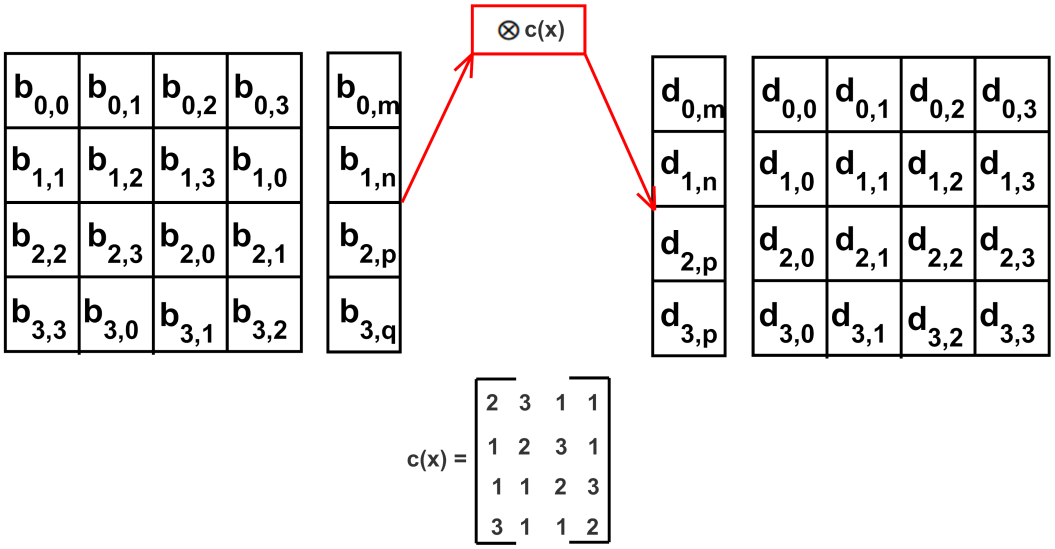
Obrázek 4.3: Operace SubBytes.

- **ShiftRows** – v tomto kroku jsou bajty každého řádku stavové matice cyklicky posunuty do leva, viz obrázek 4.4. Počet míst, o který je posun proveden se pro jednotlivé řádky liší. Cílem tohoto kroku je zabránění existence lineárně nezávislých sloupců,

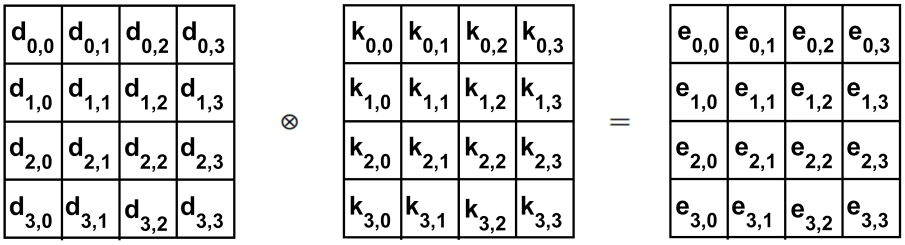


Obrázek 4.4: Operace ShiftRows.

- **MixColumns** – v tomto kroku je každý sloupec stavové matice vynásoben polynomem c(x)=3x^3+x^2+x+2 mod x^4+1. Implementuje se pomocí XOR. Společně s operací ShiftRows zajišťuje difuzi šifry, tedy závislost každého bitu prostého textu a klíče na každý bit šifrovaného textu. Tento krok je znázorněn na obrázku 4.5,
- **AddRoundKey** – každý bajt stavové matice je zkombinovaný s podklíčem, viz obrázek 4.6. Podklíč je určen pomocí klíčového plánovacího algoritmu a je vytvářen pro každou iteraci.



Obrázek 4.5: Operace MixColumns.



Obrázek 4.6: Operace AddRoundKey.

Dešifrování je provedeno inverzí jednotlivých operací v opačném pořadí než šifrování [22]:

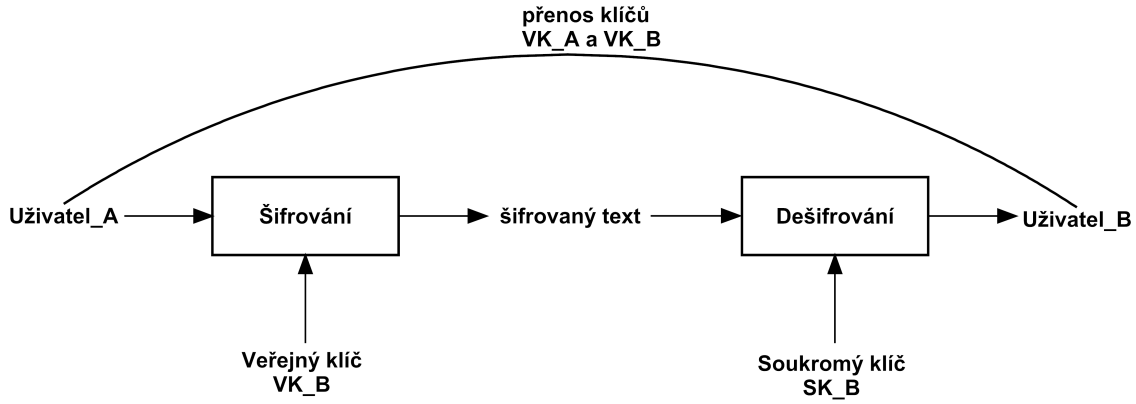
- **InvAddRoundKey** – XOR je operace inverzní sama k sobě, stačí sečíst jednotlivé bajty stavové matice s odpovídajícími podklíči,
- **InvMixColumn** – inverze je provedena vynásobením inverzním polynomem c^{-1}(x) = $11x^3$+$13x^2$+9x+14 mod x^4+1,
- **InvShiftRows** – inverze se provádí cyklickým posuvem bajtů doprava,
- **InvSubBytes** – inverze se provádí pomocí vyhledávání v tabulce Rijndael-S.

4.3.3 Asymetrické šifrování

Na rozdíl od symetrického šifrování se pro šifrování a dešifrování u asymetrického šifrování používají vždy dva odlišné klíče, veřejný klíč, který je dostupný všem a soukromý, který je znám pouze vlastníkovi klíče. Princip šifrování ukazuje obrázek 4.7. Pokud je zpráva zašifrována veřejným klíčem, lze ji dešifrovat pouze odpovídajícím soukromým klíčem, navíc není možné z veřejného klíče odvodit klíč soukromý.

Například pokud uživatel A chce poslat šifrovanou zprávu uživateli B, je postup tohoto spojení následující [24]:

- uživatel B musí vygenerovat dvojici klíčů, veřejný klíč VK-B a soukromý klíč SK-B,
- uživatel B si uloží klíč SK-B na bezpečné úložiště, například pevný disk nebo čipovou kartu,
- nyní uživatel B distribuuje klíč VK-B k uživateli A,
- uživatel A po obdržení klíče VK-B tímto klíčem zašifruje zprávu a odesílá ji uživateli B,
- uživatel B dešifruje přijatou šifrovanou zprávu klíčem SK-B a získá původní zprávu.



Obrázek 4.7: Algoritmus asymetrického šifrováni.

Tato metoda šifrování odstraňuje problém s bezpečným předáváním sdíleného klíče, který existuje u symetrického šifrování. Hlavní nevýhoda těchto algoritmů je vysoká výpočetní složitost a s tím spojená nízká rychlost šifrování. V praxi se asymetrické šifry používají především k distribuci symetrických klíčů. Další problém představuje přenos veřejných klíčů, které sice nemusí být utajeny, ale je potřeba zajistit jejich integritu, tedy

že během přenosu nedošlo k žádným úpravám. K zajištění integrity se využívají digitální podpisy a hashovací funkce. Mezi zástupce asymetrického šifrování patří algoritmy RSA (Rivest, Shamir, Adleman), DH (Diffie-Hellman) a ECC (Elliptic Curve Cryptography). O algoritmu ECC se uvažuje jako o možné alternativě implementace obousměrné autentizace v systémech EPON a 10GEPON [23].

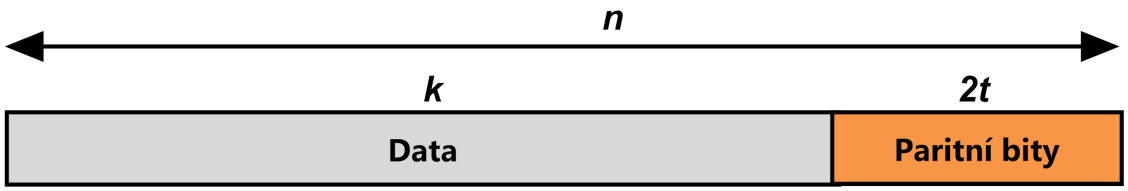
4.4 Kódování FEC

FEC (Forward Error Correction) je označení pro metodu, která se v telekomunikačních sítích používá k detekci a případné opravě chyb vzniklých při přenosu dat. Díky této technice je umožněn spolehlivý přenos data s malou chybovostí, který by jinak vedl k jejich opětovnému odeslání. Přítomnost FEC kódování v PON systémech znamená snížení užitečné přenosové rychlosti přibližně o 10% [15].

Mezi korekční kódy patří Hammingův kód (HK) a Reed-Solomonův kód (RS), který je součástí všech architektur PON, vyjma EPON, kde jeho implementace není striktně vyžadována.

4.4.1 Reed-Solomon

Kód RS pracuje s bloky dat o konstantní délce, ke kterým na jejich konci přidá určitý počet redundantních (ochranných) bajtů, viz obrázek 4.8. Díky těmto redundantním bajtům může dekodér provést detekci a opravu chyb a obnovit tak původní data. Reed-Solomonovy kódy se označují RS(n, k), kde k označuje počet bajtů vstupujících do dekodéru a n značí velikost zprávy vystupující z dekodéru. Počet redundantních bajtů v jednom bloku je $n - k$. RS dekodér je schopný opravit t chyb, přičemž platí $2t = n - k$. Pokud vezmeme jako příklad nejběžnější kód RS(255,239) tak se každý přenášený blok skládá z 239 bajtů dat a 16 bajtů parity. Tímto kódem jsme tedy schopni v jednom bloku opravit chyby o velikosti až 8 bajtů [25].



Obrázek 4.8: Struktura přenášeného bloku.

4.5 Autentizace

Autentizace je proces k ověření jedné nebo obou stran navázaného spojení. V systémech PON se můžeme setkat se třemi modely autentizace.

4.5.1 Autentizace podle hesla

Tento typ autentizace byl implementován v technologii APON. Jedná se o velmi jednoduchý typ jednostranného ověření jednotky ONU.

ITU-T G.983 popisuje tuto autentizaci jako výměnu hesel. Heslem může být sériové číslo jednotky ONU anebo správcem sítě definovaná hodnota. Jednotka OLT odešle požadavek o vystavení hesla některé z připojených jednotek ONU a tato jednotka postupně odešle své heslo třikrát. Pokud OLT přijme tři identická hesla, považuje toto heslo za správné a postupuje k procesu ověření. Existují dvě metody ověření. U první metody má jednotka OLT správcem sítě přednastavenou tabulku s uloženými hesly jednotlivých koncových jednotek ONU a ověřuje pouze shodu. U druhé metody jednotka OLT nemá uloženou tabulku s hesly a za důvěryhodné heslo považuje první, které koncová jednotka odešle během připojování do sítě [8].

4.5.2 Autentizace podle registračního ID

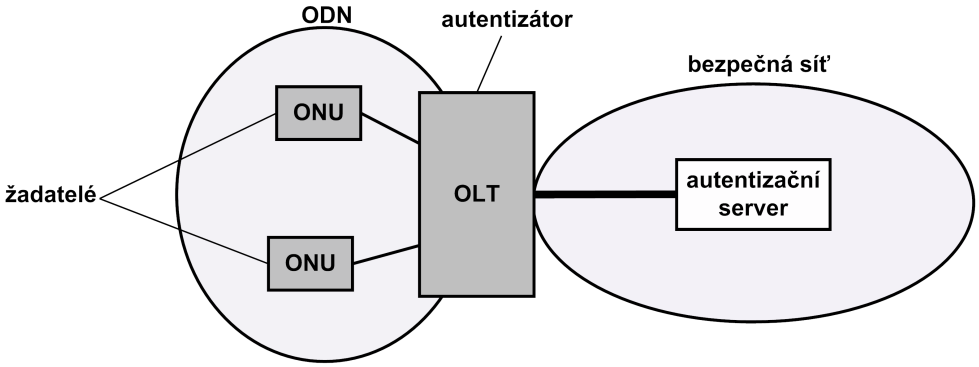
Tímto modelem autentizace je možné ověřit opět pouze jednotku ONU směrem k jednotce OLT a ne naopak. Principem je tento model velmi podobný autentizaci z technologie APON. Podpora této metody ověření je v v technologiích GPON a XG-PON povinná. Pro správnou funkcionalitu je potřeba splnit dva požadavky. Za prvé musí být registrační ID zákazníkovi předem přiděleno na úrovni managementu a za druhé musí být toto registrační ID správcem sítě vloženo do jednotky OLT i ONU.

Během aktivování jednotky ONU do sítě tato jednotka vyšle na žádost jednotky OLT své registrační ID ve formě registrační služební zprávy PLOAM. Jednotka OLT po obdržení registračního ID toto ID porovná se svým záznamem a pokud je vše v pořádku, povolí jednotce ONU přístup k síti. V opačném případě jej zablokuje. Pro větší ochranu jednotka OLT může požadovat reautentizaci kterékoliv jednotky ONU kdykoliv během navázaného spojení, postup této opakované autentizace je stejný [9], [11].

4.5.3 Autentizace IEEE 802.1X

Tento model autentizace umožňuje oboustranné ověření identity jednotek ONU a OLT. Obvykle bývá implementován do systémů EPON, 10GEPON a rovněž je součástí XG-PON systémů, kde je ale jeho aktivace pouze volitelná. [3]

Protokol IEEE 802.1x je používaný na spojové vrstvě pro autentizaci, založené na řízení přístupu k portu. Mechanismus autentizace 802.1x se skládá ze tří částí, viz obrázek 4.9. Jednotka ONU je v roli žadatele (supplicant), jednotka OLT je v roli autentizátora (authenticator) a poslední částí je autentizační server, entita poskytující autentizační informace autentizátoru, se kterým musí autentizátor udržovat fyzicky nebo logicky zabezpečené spojení. Komunikace mezi jednotkou OLT a autentizačním serverem je obvykle (ne nutně) řešena pomocí protokolu RADIUS (Remote Authentication Dial In User Service) [11].



Obrázek 4.9: Model autentizace IEEE 802.1x.

IEEE 802.1x nedefinuje které konkrétní prvky jsou používané k ověření identity, ale definuje enkapsulaci protokolu EAP (Extensible Authentication Protocol), který podporuje velké množství těchto prvků. Existuje několik druhů autentizací EAP např. EAP-TLS, EAP-MD5, PEAP, atd. kde každý může využívat jiný ověřovací prvek. Těmito prvky můžou být veřejné klíče, různé formáty hesel, čipové karty apod. [26]. Aby byla zajištěna interoperabilita, je nutné u všech jednotek OLT i ONU použít jeden typ autentizace. U systémů XG-PON byla zvolena autentizace typu EAP-GPSK (EAP-Generalized Pre-Shared Key), která jako ověřovací prvek využívá předem sdílený klíč. Klíč je uživateli sdělen například přes telefon nebo je uveden ve smlouvě a k zprovoznění stačí už jen tento klíč uložit do jednotky ONU na straně uživatele a do autentizačního serveru na straně poskytovatele [11].

[3] Podporu autentizace typu 802.1x má rovněž WDM-PON OLT jednotka, s kterou bylo provedeno praktické měření. [30]

Samotný proces autentizace je už potom velmi podobný autentizacím popsaným výše. Při připojení jednotky ONU do sítě vyšle jednotka OLT požadavek o vystavení identifikátoru a přiděleného hesla. Jednotka ONU identifikátor a heslo odešle a jednotka OLT tyto údaje po zpracování předá autentizačnímu serveru. Autentizační server buď to potvrdí pravost identifikace a povolí jednotce ONU přístup do sítě anebo přístup zablokuje [27].

5 Praktické měření

V této části práce jsou prakticky ověřena bezpečnostní rizika spojená s provozem systémů WDM-PON, respektive WDM/TDM-PON. Měření bylo provedeno pomocí vybavení dostupného v laboratoři katedry telekomunikací (KAT440) VŠB-TUO.

Hlavním cílem měření je ověřit případnou existenci přeslechů mezi sousedními kanály, při využití metody vydělování vlnových délek pomocí odbočnice AWG.

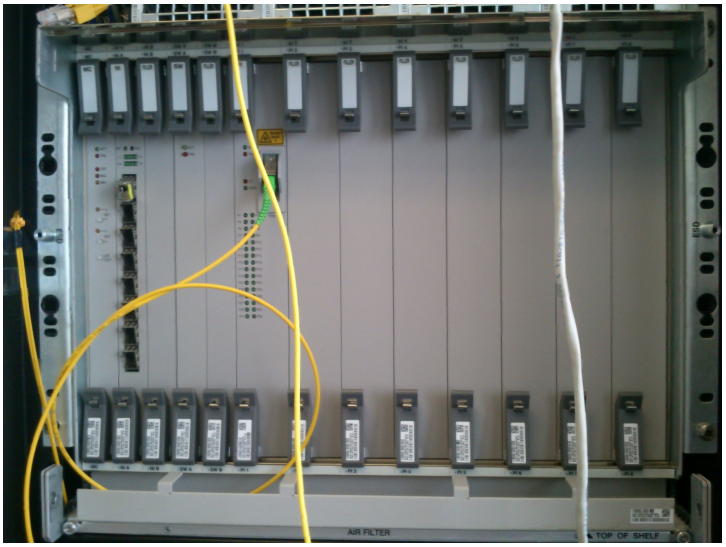
5.1 Popis měřícího pracoviště a použité přístroje

Pracoviště se nachází v laboratoři optických přístupových sítí katedry 440, v budově N, učebně 311. Hlavní rozvaděč je propojený s jednotlivými lavicemi učebny pomocí dvojice optických vláken typu G.652D a dvojice vláken typu G.657.B3. Vlákna jsou ukončená v panelech zásuvek pro rovný konektor SC (PC) a šikmý konektor SC (APC). V panelech se rovněž nacházejí dva porty pro připojení kabelů UTP s konektory RJ45.

Pro měření byly použity aktivní a pasivní prvky distribuční sítě, konkrétně jednotka OLT LG-Nortel EAST 1100 (Release 3), pasivní odbočnice AWG LG-Nortel WPF 1132C, tři kusy koncových jednotek ONT LG-Nortel EARU 1112 a pasivní rozbočovač. Jednotka OLT, odbočnice a rozbočovač jsou umístěny v hlavním rozvaděči, jednotky ONT byly položeny na lavici. Dalším použitým přístrojem byl optický spektrální analyzátor EXFO FTB-400 s modulem FTB-5240S.

WDM-PON LG-Nortel EAST 1100

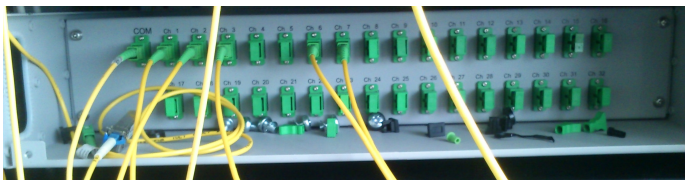
LG-Nortel EAST (Ethernet Access Service Terminal) 1100 je hlavní stanice určená pro instalaci do hlavních rozvoden. Zařízení je modulární a umožňuje snadné rozšíření kapacity při minimálních nákladech. Je vhodné pro datové služby, které se dnes hojně využívají, například VoIP, IPTV, VoD a vysokorychlostní internet. Bezpečnostním prvkem je autentizace typu 802.1x využívající protokol RADIUS. Datová komunikace ke každému koncovému zařízení dosahuje až 1 Gbit/s. Integrovanými prvky jsou dva L2/L3 switche, osm portů pro karty obsluhy koncových zařízení a diagnostická karta systému dohledu [30].



Obrázek 5.1: LG-Nortel EAST 1100.

LG-Nortel WPF 1132c

LG-Nortel WPF (Wavelength Passive Filter) 1132c je zařízení pro multiplexování a demultiplexování optického signálu na trase mezi hlavní stanicí OLT (LG-Nortel EAST 1100) a koncovými zařízeními ONT (LG-Nortel EARU 1112). Tento filtr je schopný odfiltrovat jednotlivé vlnové délky na příslušné výstupy a tím tyto vlnové délky od sebe izolovat. Jedná se o pasivní filtr AWG, na který je možné připojit až 32 koncových jednotek [31].

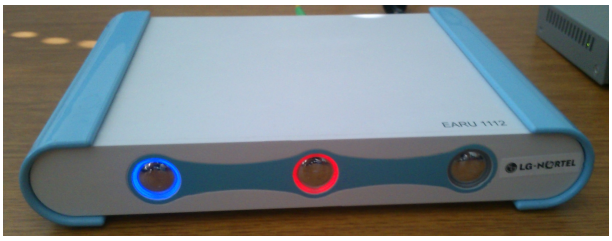


Obrázek 5.2: LG-Nortel WPF 1132c.

LG-Nortel EARU 1112

LG-Nortel EARU (Ethernet Access Residential Unit) 1112 je koncová ONT jednotka spadající do kategorie malých koncových zařízení a je určená především pro domácnosti. Zajištěna je podpora standardních datových služeb a QoS. Bezpečnostní prvky nejsou v technických specifikacích výrobce uvedeny. Zařízení obsahuje čtyři porty pro konektory RJ45 a jeden optický port SC (APC). Největší předností je kompatibilita v celém vlnovém spektru. Maximální podporovaná rychlost této jednotky je v obou směrech

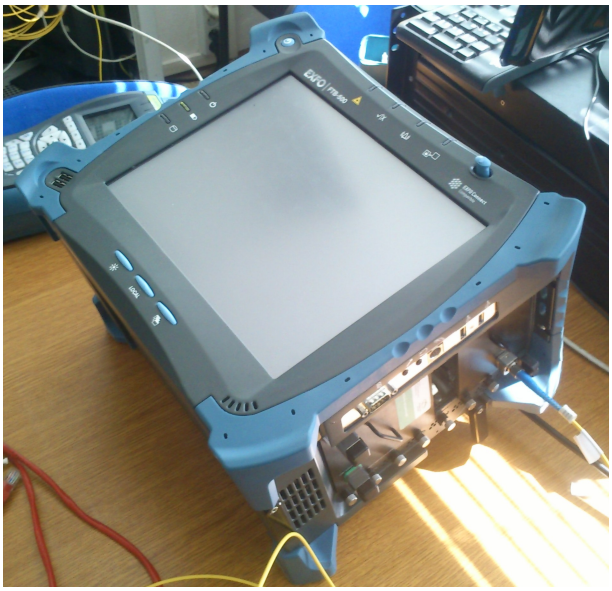
100 Mbit/s [32].



Obrázek 5.3: LG-Nortel EARU 1112.

EXFO FTB-400

EXFO FTB-400 je univerzální měřicí přístroj z dílny kanadského výrobce. Hlavní výhoda tohoto systému spočívá v intuitivním ovládání, jednoduchém managementu a rychlém převodu dat do formátu pdf. Součástí přístroje je modul FTB-5240S. Tento modul je analyzátor optického spektra, který umožňuje měření vlnových délek. (základní nástroj DWDM) [33].



Obrázek 5.4: EXFO FTB-400.

5.2 Konfigurace zařízení

Konfiguraci zařízení WDM-PON LG-Nortel EAST 1100 je možné realizovat dvěma způsoby, buď'to přes příkazový řádek CLI (Command Line Interface) nebo pomocí grafic-

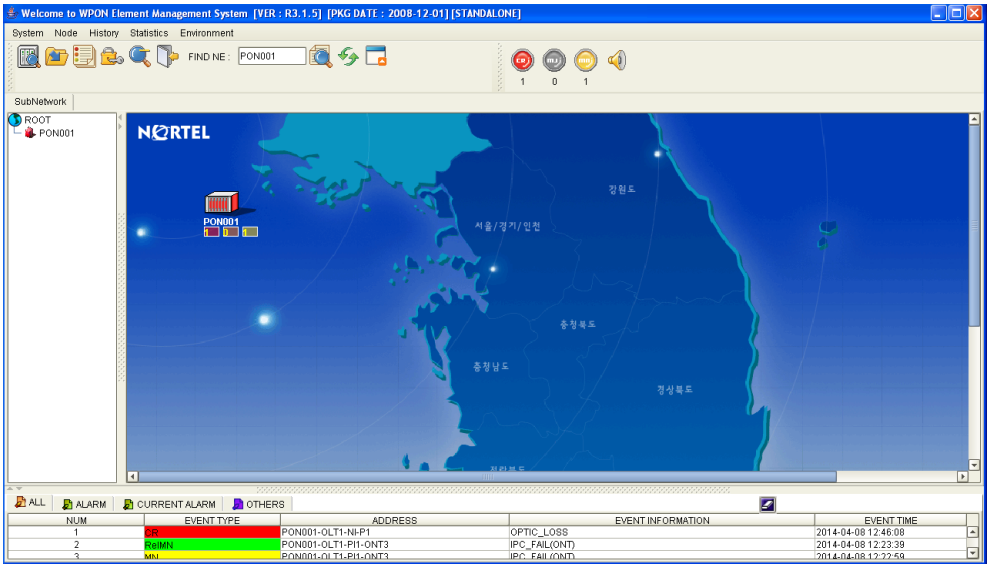
kého rozhraní. Já jsem zvolil variantu s grafickým rozhraním, které je rychlejší, pohodlnější a umožňuje nastavení funkcí, které jsou nutné pro mé měření. Software EA Manager už byl nainstalován na stolním počítači nacházejícím se v učebně a stačilo už tedy pouze propojit počítač s portem EMS (Element Management Systém) na jednotce OLT pomocí kabelu UTP. Pro úspěšné navázání spojení je nutné, aby se port EMS i počítač nacházel ve stejné síti. Port EMS měl přednastavenou ip adresu 192.168.142.105 a na počítači byla přednastavena ip adresa z téže sítě takže nebylo potřeba žádných úprav.

Obrázek 5.5: Přihlašovací okno EA Manageru.

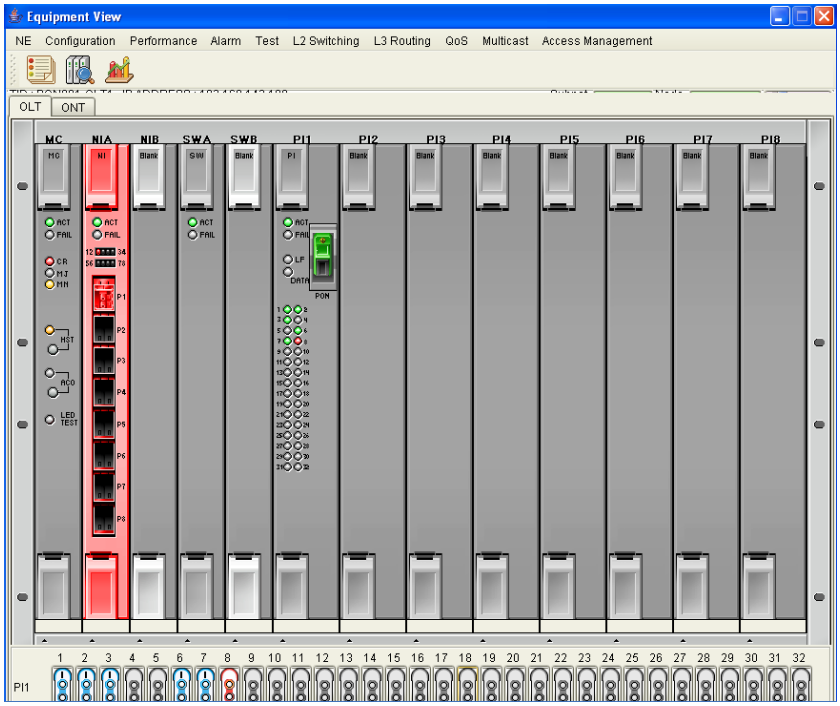
Po spuštění programu EA Manager se objeví přihlašovací okno viz obrázek 5.5. Zde je možné v kolonce *SERVER IP* změnit IP adresu nastavenou na portu EMS. Nutné je vyplnit přihlašovací údaje *USER ID – admin* a *PASSWORD – admin*. Obě hodnoty jsou implicitní a jsou uvedeny v manuálu. Po úspěšném nalogování se nám objeví úvodní okno EA Manageru zobrazené na obrázku 5.6.

Nyní je nutné provést synchronizaci s jednotkou OLT. Toho dosáhneme kliknutím na *System -> Synchronization DB*. Po úspěšné synchronizaci se můžeme pustit do konfigurace potřebných nastavení. Dvojklikem na ikonku PON001 se zobrazí okno se zásuvnými kartami, obrázek 5.7.

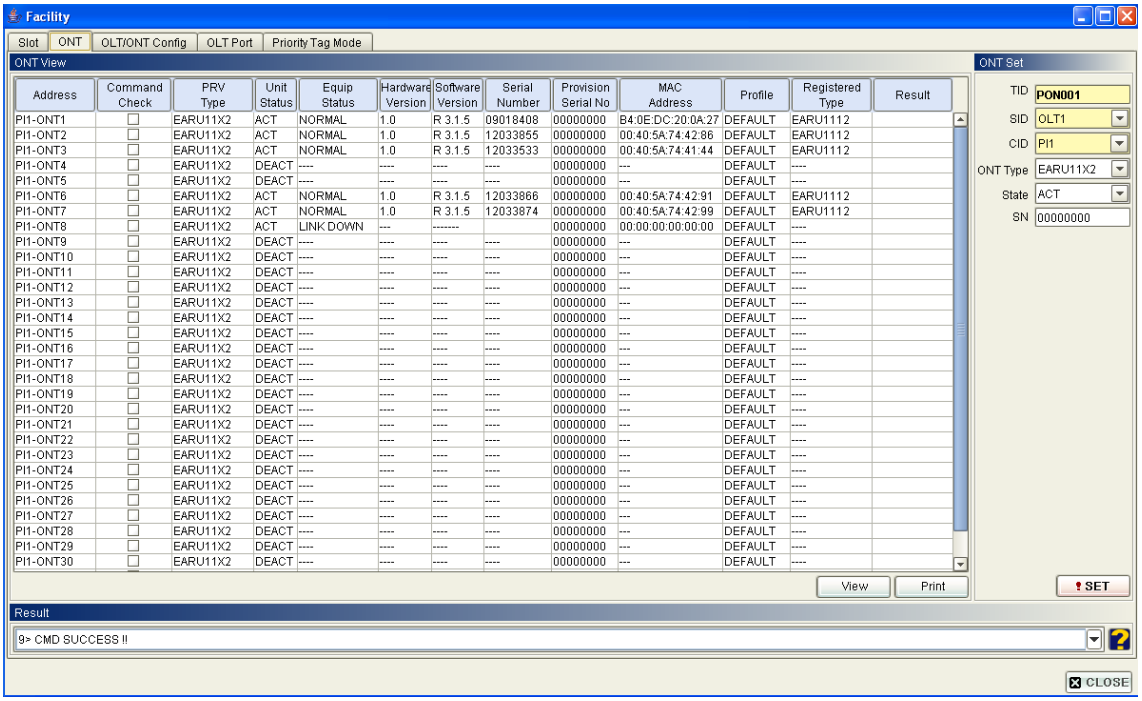
Po kliknutí na *Configuration -> Facility -> ONT* se nám zobrazí okno *Facility*, kde můžeme podle potřeby aktivovat nebo deaktivovat jednotlivé koncové jednotky viz obrázek 5.8. Ačkoliv EA Manager umožňuje nastavení daleko více parametrů a funkcí, pro naše měření je toto dostačující.



Obrázek 5.6: Úvodní okno EA Manageru.



Obrázek 5.7: Okno se zásuvnými kartami (Equipment View).

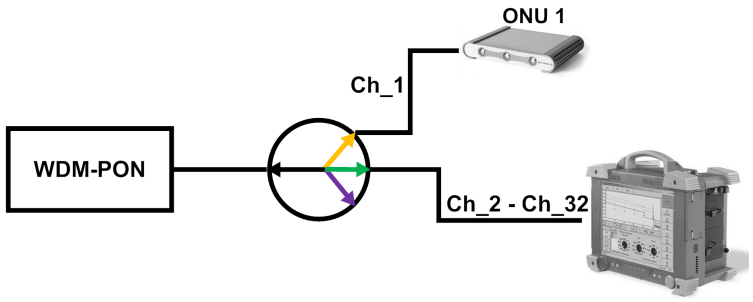


Obrázek 5.8: Okno s možností aktivace a deaktivace koncových jednotek (Facility).

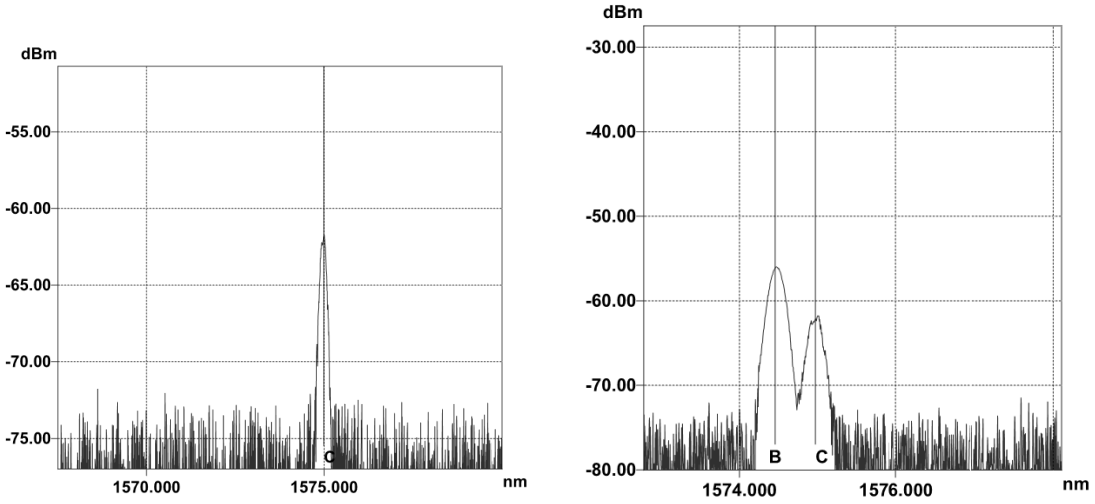
5.3 Spektrální analýza navržených topologií

Případnou existenci přeslechů mezi sousedními kanály a s tím spojenou hrozbu odposlechu, blíže popsanou v kapitole 5.2, odhalíme spektrální analýzou sítě. Měření se uskutečnilo pomocí spektrálního analyzátoru EXFO FTB-400/5240S.

V prvním bodě měření byla do filtru AWG připojena pouze jedna jednotka ONU. Optický spektrální analyzátor jsem poté postupně připojoval na všechny ostatní, neobsazené kanály AWG filtru a pozoroval, kdy na spektru dojde k nějaké změně. Použitá topologie je vyobrazena na obrázku 5.9.



Obrázek 5.9: Topologie č. 1.



(a) Neaktivní jednotka na kanálu 1. **(b)** Aktivní jednotka na kanálu 1.

Obrázek 5.10: Spektrum kanálu č. 2 před a po aktivaci jednotky na kanálu č. 1.

Na obrázku 5.10a vidíme spektrum naměřené na kanálu č. 2, když byla jednotka ONU na kanálu č. 1 deaktivovaná. Naměřená špička označená značkou C je širokopásmový zdroj světla, sloužící koncovým jednotkám k zachycení na přidělenou vlnovou délku viz princip Fabry-Perot WDM-PON v kapitole 3.3. Na obrázku 5.10b vidíme totéž spektrum, avšak tentokrát byla ONU jednotka na kanálu č. 1 aktivní. Předpoklad, že dochází k přenosu signálu malé úrovně ze sousedního kanálu se nám tedy potvrdil, přeslech je patrný na první pohled. Protože nám analyzátor parametry tohoto přeslechu nezměřil automaticky, pravděpodobně z důvodu nízkého výkonu signálu, bylo potřeba jej změřit manuálně. No obrázku jsou vidět značky B a C, které byly k tomu účelu použity. Tímto manuálním měřením jsme schopni zjistit pouze vlnovou délku a výkon signálů. Parametry jako je výkon šumu nebo SNR touto metodou nezískáme. Zjištěné parametry jsou uvedeny v tabulce 5.1.

Špicka	Vlnová délka (nm)	Výkon (dBm)
B	-	-
C	1574,967	-62,01

(a) Neaktivní jednotka na kanálu č. 1.

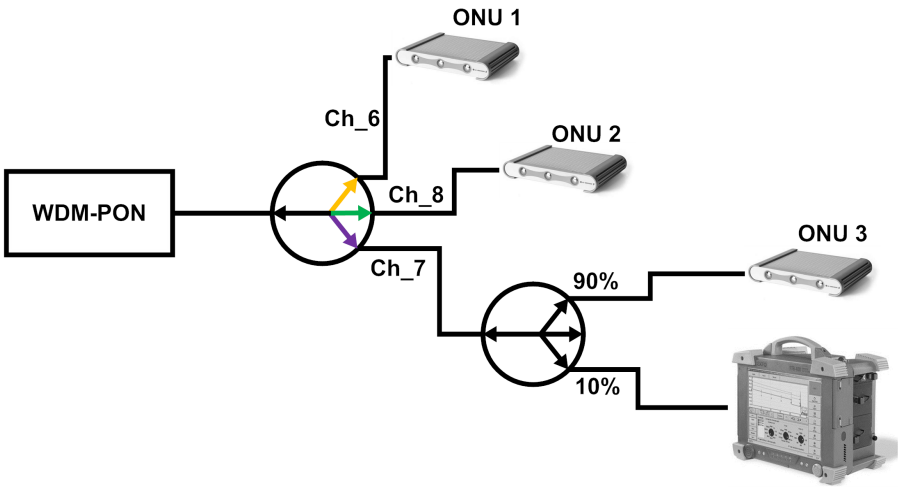
Špicka	Vlnová délka (nm)	Výkon (dBm)
B	1574,456	-56,10
C	1574,967	-62,19

(b) Aktivní jednotka na kanálu č. 1.

Tabulka 5.1: Parametry spektra na kanálu č.2 před a po aktivaci jednotky na kanálu č. 1.

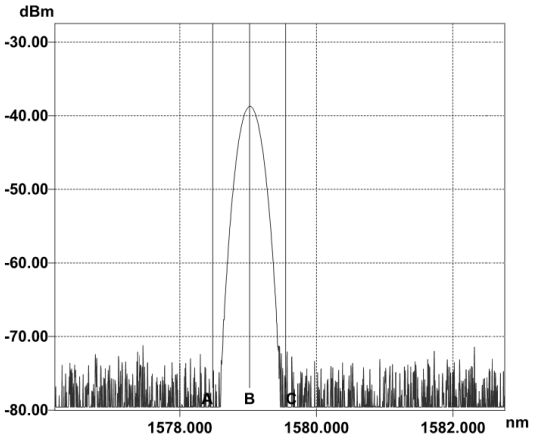
Abychom se ujistili, že se nejedná o náhodný jev, připojili jsme jednotku ONU postupně i na ostatní kanály AWG filtru a postup měření spektrálním analyzátorem opakovali. Výsledky těchto měření jsou uvedeny v příloze A. Zjistili jsme, že se o náhodný jev nejedná, přeslechy jsou patrné na všech takto měřených kanálech a úroveň těchto přeslechů je srovnatelná.

V druhém bodě měření jsme lehce upravili topologii tak, aby více odpovídala skutečnému provozu. Použitá topologie je zobrazena na obrázku 5.11. V tomto případě jsme pro měření přeslechů vybrali náhodně kanál č. 7. Cílem bylo zjistit, které signály je jednotka ONU na tomto kanálu teoreticky schopna zpracovat. V zapojení bylo potřeba použít optický rozbočovač s dělícím poměrem 1:2, kdy na jeden výstup bylo přivedeno 90% vstupního signálu, který dále pokračoval do jednotky ONU a na druhý výstup zbývajících 10% signálu, který pokračoval do spektrálního analyzátoru. Na kanál č. 6 a 8 AWG filtru byly připojeny další dvě jednotky ONU, jejichž signály jsme se snažili zachytit.

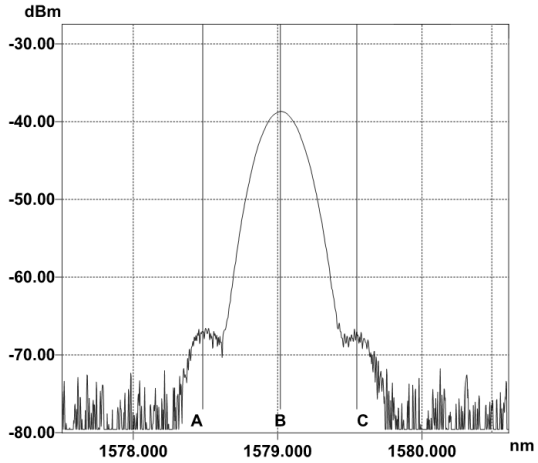


Obrázek 5.11: Topologie č. 2.

Na obrázku 5.12a vidíme spektrum aktivní jednotky ONU na kanále č. 7 před aktivací jednotek na kanálech č. 6 a 8. Spektrum po aktivaci těchto jednotek ukazuje obrázek 5.12b. Existenci přeslechů jsme i tímto měřením potvrdili. Parametry přeslechů udává tabulka 5.2, hodnota vložného útlumu optického rozbočovače je již v těchto hodnotách započítána.



(a) Neaktivní jednotky na kanálech č. 6 a 8.



(b) Aktivní jednotky na kanálech č. 6 a 8.

Obrázek 5.12: Spektrum naměřené na jednotce ONU připojené na kanálu č. 7.

Špicka	Vlnová délka (nm)	Výkon (dBm)
A	-	-
B	1579,024	-28,55
C	-	-

(a) Neaktivní jednotky na kanálech č. 6 a 8.

Špicka	Vlnová délka (nm)	Výkon (dBm)
A	1578,482	-56,89
B	1579,024	-28,52
C	1579,548	-56,91

(b) Aktivní jednotky na kanálech č. 6 a 8.

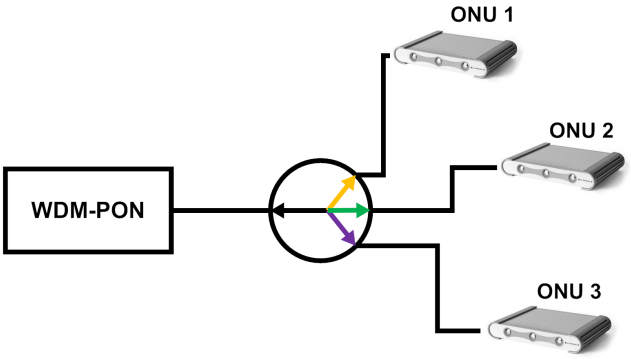
Tabulka 5.2: Parametry spektra na jednotce ONU připojené na kanálu č. 7 před a po aktivaci jednotek na kanálech č. 6 a 8.

Po porovnání výsledků z obou bodů měření je vidět, že v obou případech přeslechy dosahují úrovně přibližně -57 dBm. Z toho je patrné, že použitá topologie nemá na úroveň těchto přeslechů vliv. Přeslechy jsou způsobeny technickým nedostatkem respektive nepřesností filtru AWG při vydělování vlnových délek.

5.4 Simulace v programovém prostředí Optiwave

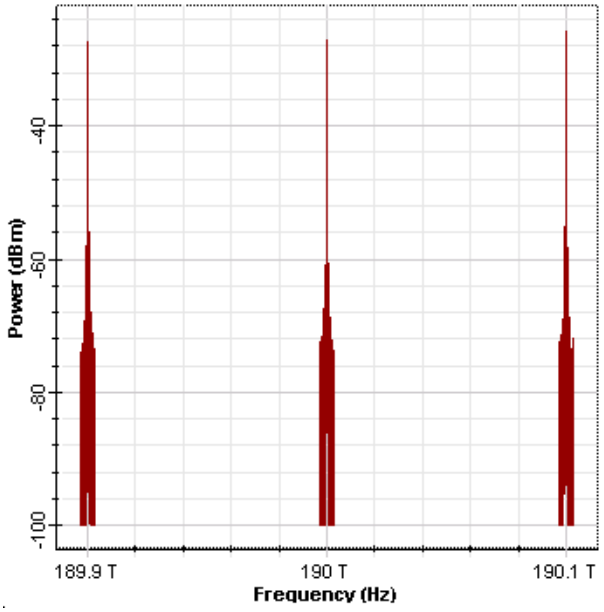
Výsledky z praktického měření jsem použil pro simulaci v programu Optiwave. V tomto simulačním prostředí nejsme omezeni dostupností hardwarových prvků a máme k dispozici větší množství nástrojů pro analýzu signálu. V našem případě se nám velmi hodí např. diagram oka, pomocí kterého zjistíme, zdali je úroveň přeslechů dostatečná pro rekonstrukci čitelné informace. Bloková schémata použitých topologií v programu Optiwave jsou zobrazena v příloze C.

Nejprve jsem sestavil topologii použitou v druhém bodě praktického měření viz obrázek 5.13. Topologii jsem lehce upravil tím, že jsem odstranil pasivní rozbočovač. Rozbočovač není v simulaci potřeba, protože spektrální analyzátor můžu umístit na libovolné výstupy na přímo.



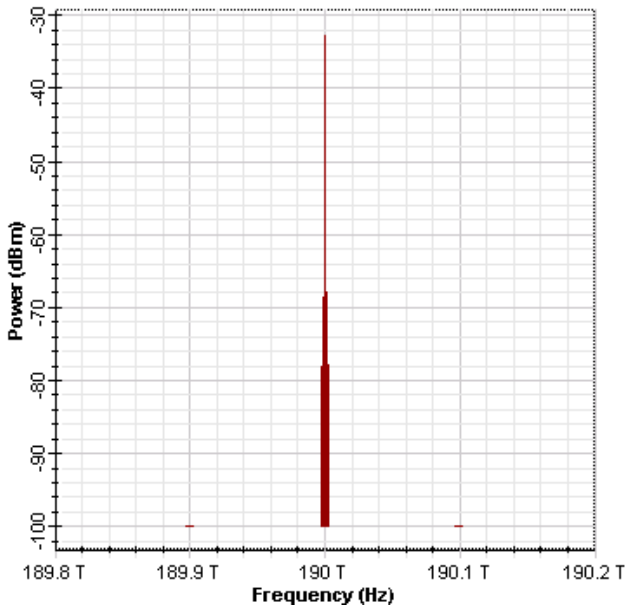
Obrázek 5.13: Topologie č.1 v prostředí Optiwave.

Na obrázku 5.14 je vidět spektrum sestupného směru před vstupem do filtru AWG.



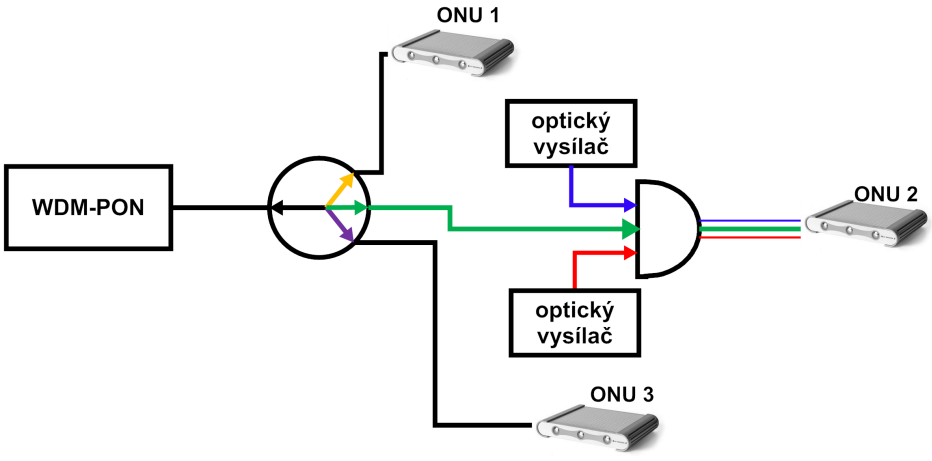
Obrázek 5.14: Spektrum před filtrem AWG.

Na obrázku 5.15 je zobrazen odfiltrovaný kanál, vyvedený z filtru AWG do jednotky ONU 2. Jak je vidět, okolní kmitočty nebyly propuštěny, což značí ideální funkci filtru AWG.



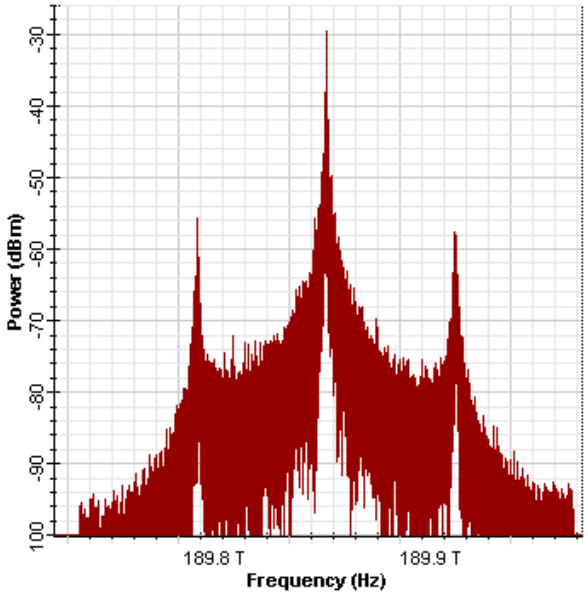
Obrázek 5.15: Spektrum za filtrem AWG na jednotce ONU 2.

Jak jsme ale zjistili praktickým měřením, v reálných podmínkách takto ideálně filtr AWG nefunguje. Na obrázku 5.16 je vidět topologie, pomocí které jsme nasimulovali reálnou situaci z obrázku 5.12b. Za filtr AWG jsem připojil optický sdružovač se sdružovacím poměrem 3:1. Na jeden vstup sdružovače jsem přivedl signál z filtru AWG. Na ostatní dva vstupy jsem připojil optické vysílače, které jsem nastavil tak, aby nám simulovaly přeslechy ze sousedních kmitočtů s parametry uvedenými v tabulce 5.2b.



Obrázek 5.16: Topologie pro simulaci reálné situace.

Obrázek 5.17 zobrazuje spektrum naměřené na výstupu sdružovače, tedy spektrum které vstupuje do koncové jednotky ONU 2. Obrázek 5.18 ukazuje diagram oka změřený na této jednotce. Na diagramu je otevření oka ideální s minimálním zašuměním, což značí kvalitní příjem.



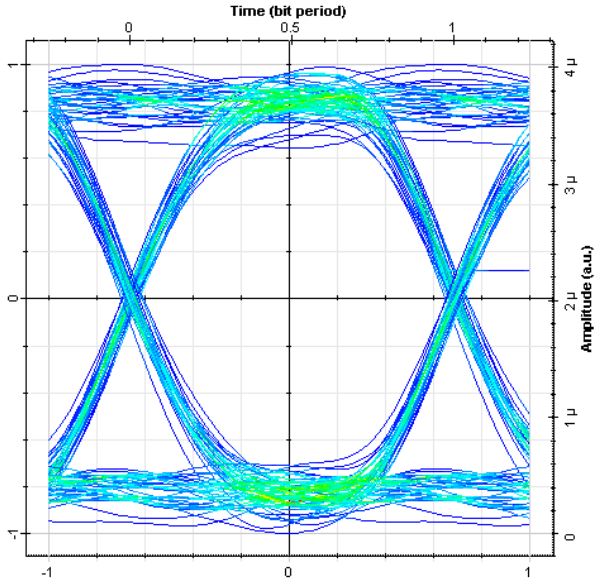
Obrázek 5.17: Optické spektrum na výstupu sdružovače.

Parametry signálů naměřeného spektra jsou uvedeny v tabulce 5.3. S nastavením kmitočtů, respektive vlnových délek u optických vysílačů nebyl problém. Trochu složitější bylo nastavení správných úrovní signálů, které se sice nepovedlo nastavit úplně přesně, ale vzniklá odchylka je zanedbatelná a parametry jsou s parametry v tabulce 5.2b srovnatelné.

Tabulka 5.3: Parametry signálů spektra na výstupu sdružovače.

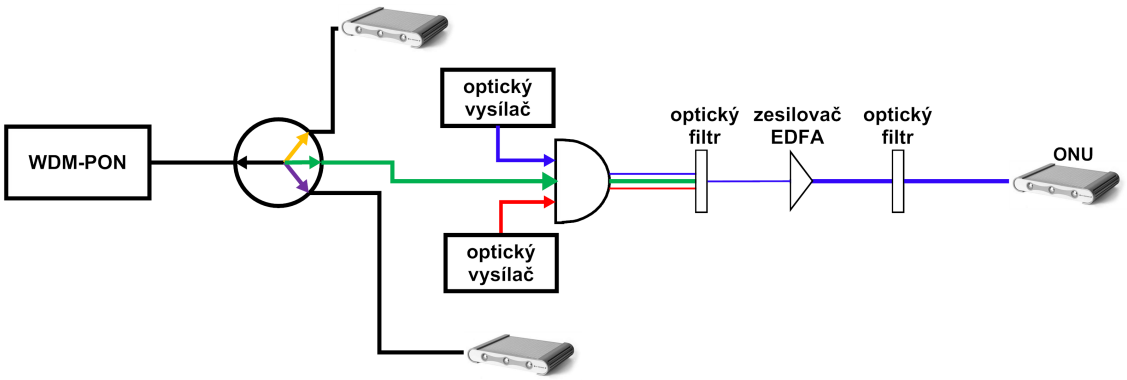
Špicka	Vlnová délka (nm)	Kmitočet (THz)	Výkon (dBm)
1	1578,482	189,92453	-56,72
2	1579,024	189,85934	-29,34
3	1579,548	189,79363	-57,16

Nyní, když jsem měl připravenou simulaci reálné situace jsem mohl provést pokus, který v laboratorních podmínkách nebylo možné provést, z důvodu nedostupnosti po-



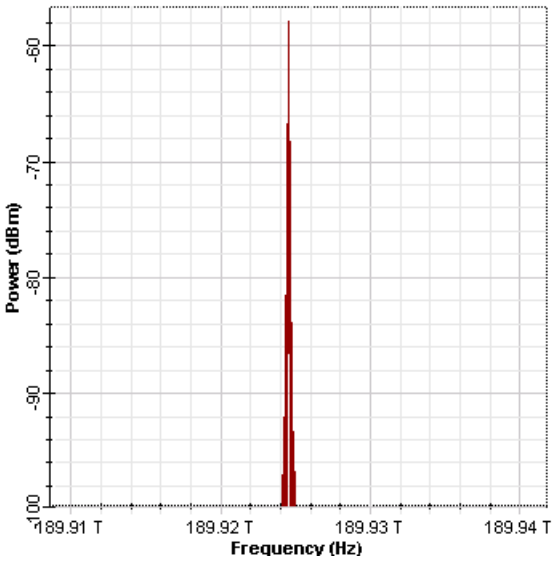
Obrázek 5.18: Diagram oka jednotky ONU 2.

třebného hardwaru. Cílem tohoto pokusu je zjistit, zdali se dá realizovat odposlech přenášených dat, s využitím přeslechů ze sousedních kanálů. Princip je zobrazen na obrázku 5.19. Spočívá v odfiltrování jednoho z přeslechů, jeho následném zesílení a vyhodnocení kvality pomocí diagramu oka na jednotce ONU.



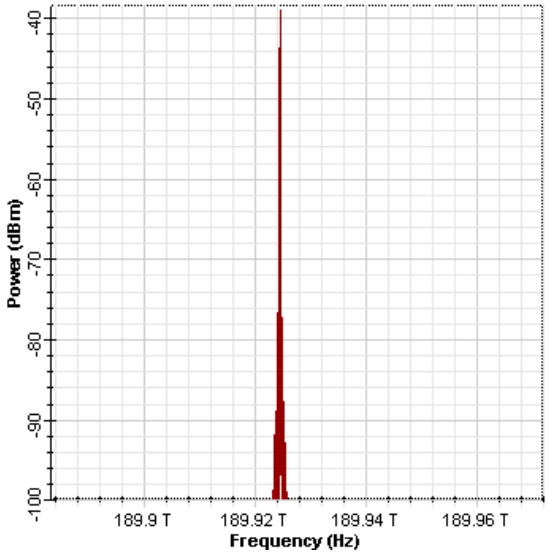
Obrázek 5.19: Topologie pro simulaci odposlechu s využitím přeslechu.

Na výstup sdružovače jsem připojil optický filtr, kterým jsem si přeslech na vlnové délce 1578,482 nm odfiltroval, viz obrázek 5.20.

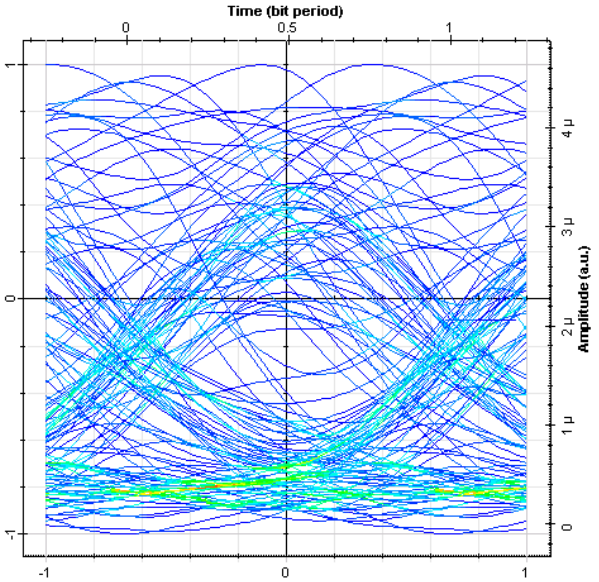


Obrázek 5.20: Odfiltrovaný signál na vlnové délce 1578,482 nm.

Již odfiltrovaný signál jsem pomocí zesilovače EDFA (Erbium Doped Fibre Amplifier) zesílil o 20 dBm, což je běžná hodnota skutečných zesilovačů tohoto typu. Takto zesílený signál jsem nechal projít dalším filtrem, abych odstranil všechen nežádoucí šum, který mohl aplikací zesilovače vzniknout. Zesílený a odfiltrovaný signál je zobrazen na obrázku 5.21. Tento signál poté dále pokračoval do koncové jednotky ONU, kde jsem provedl měření diagramem oka viz obrázek 5.22.



Obrázek 5.21: Odfiltrovaný a zesílený signál na vlnové délce 1578,482 nm.



Obrázek 5.22: Diagram oka zesíleného signálu.

Simulací jsme zjistili, že odposlech přenášených dat skrze přeslechy ze sousedních kanálů není možný. Kvalita ani zesíleného signálu není dostatečná pro čitelnou rekonstrukci přenášené zprávy.

Závěr

Tato bakalářská práce se zabývá bezpečností a bezpečnostními riziky spojenými s provozem pasivních optických sítí PON, současné i budoucí generace.

V sítích současné generace, obecně označované jako TDM-PON, je existence bezpečnostních rizik nezpochybnitelná. Hlavními riziky jsou odposlech přenášených dat, impersonace síťových jednotek a odepření služby. Tato bezpečnostní rizika pochází ze samotného principu všesměrové povahy šíření signálu od centrální jednotky ke koncovým jednotkám a ze sdílení přenosového média. Závažnost jednotlivých rizik je potřeba posuzovat pro každou technologii TDM-PON individuálně, protože každá využívá jiné bezpečnostní mechanismy. U technologií standardu ITU-T míra zabezpečení odpovídá časovému vývoji těchto technologií. Zatímco první technologie APON/BPON poskytovala pouze malou míru zabezpečení, u nejnovější technologie XG-PON došlo k odstranění většiny nedostatků její předchůdců. U technologií vydaných v rámci standardů IEEE se míra zabezpečení nedá objektivně posoudit, neboť se bezpečnostní mechanismy mohou u různých výrobců těchto systémů lišit.

Bezpečnostní rizika v sítích nové generace se odvíjí od použité architektury. U variant hybridní WDM/TDM-PON, nebo WDM-PON s pasivním rozbočovačem jsou z důvodu všesměrového šíření signálu rizika totožná s riziky technologií TDM-PON. Jako nejbezpečnější se jeví technologie WDM-PON, využívající k šíření signálu filtr AWG, která mezi centrální jednotkou a koncovými jednotkami vytváří z pohledu fyzické vrstvy spojení typu bod-bod.

Jedinou hrozbou spojenou s provozem varianty WDM-PON s filtrem AWG, je možnost existence přeslechů mezi sousedními kanály, z důvodu nepřesnosti filtru AWG při vydělování vlnových délek. Ověření existence a případně míry závažnosti této hrozby bylo náplní praktické části práce.

V laboratorních podmínkách bylo provedeno měření, které existenci přeslechů potvrdilo. Naměřené úrovně výkonu signálu těchto přeslechů byly zpracovány a dále použity pro simulaci v prostředí Optiwave. Cílem simulace bylo ověřit, zdali je úroveň přeslechů dostatečná pro čitelnou rekonstrukci přenášených dat. Toho bylo dosaženo odfiltrováním signálu přeslechu, jeho zesílením a nakonec vyhodnocením pomocí diagramu oka na koncové jednotce.

Závěr této simulace je, že úroveň signálu přeslechu není pro rekonstrukci přenášených dat dostatečná a bezpečnostní riziko spojené s odposlechem těchto přeslechů se tedy nepotvrdilo.

Literatura

[1] LAFATA, Pavel a Jiří VODRÁŽKA. *Současné a budoucí varianty pasivních optických přístupových sítí.* [online]. 2009 [cit. 2013-03-29]. Dostupné z: http://www.elektrorevue.cz/cz/clanky/komunikacni-technologie/45/soucasne-a-budouci-varianty-pasivnich-optickych-pristupovych-siti/

[2] LAFATA, Pavel a Jiří VODRÁŽKA. *Pasivní optická síť GPON.* [online]. 2009 [cit. 2014-03-29]. Dostupné z: http://access.feld.cvut.cz/view.php?cisloclanku=2009050002

[3] LAM, Cedric F. *Passive optical networks: principles and practice.* Boston: Elsevier/Academic Press, c2007, xliv, 324 p. ISBN 01-237-3853-9.

[4] K, Rajesh. *What is FTTH – Fiber To The Home and Advantages of P2P vs P2M/PON Architectures.* In: ExcITingIP [online]. 2011 [cit. 2014-03-29]. Dostupné z: http://www.excitingip.com/2496/what-is-ftth-fiber-to-the-home-advantages-of-p2p-vs-p2mpon-architectures

[5] KOUDELKA, Petr a Jan LÁTAL. *Optické přístupové sítě OAN na bázi technologie EPON a jejich integrita.* [online]. 2012 [cit. 2014-03-29]. Dostupné z: http://optice.vsb.cz/_data/FRVS/3.%20Opticke%20pristupove%20site%20OAN%20na%20bazi%20EPON%20a%20jejich%20integrita.pdf

[6] ANSARI, Nirwan a Jingjing ZHANG. *Media access control and resource allocation: for next generation passive optical networks.* Heidelberg: Springer, c2013, xvii, 111 p. SpringerBriefs in applied sciences and technology. ISBN 978-1-4614-3939-4. Dostupné z: http://www.springer.com/cda/content/document/cda_downloaddocument/9781461439387-c1.pdf?SGWID=0-0-45-1372106-p174422538

[7] Architectural concepts and alternatives for PON networks. In: AD-NET Technology [online]. [cit. 2014-03-29]. Dostupné z: http://www.ad-net.com.tw/index.php?id=998

[8] ITU-T G.983.1: Broadband optical access systems based on Passive Optical Networks (PON). [online]. 2005 [cit. 2014-03-29]. Dostupné z: http://www.itu.int/rec/T-REC-G.983.1-200501-I/en

[9] ITU-T G.984.3: Gigabit-capable Passive Optical Networks (G-PON): Transmission convergence layer specification. [online]. 2008 [cit. 2014-03-29]. Dostupné z: http://www.itu.int/rec/T-REC-G.984.3/en

[10] EFFENBERGER, Frank J. *The XG-PON System: Cost Effective 10 Gb/s Access. In: Journal of lightwave technology: a joint IEEE/OSA publication* [online]. 4. vyd., 2011 [cit. 2014-03-29]. ISSN 0733-8724. Dostupné z: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=05595476

[11] ITU-T G.987.3: 10-Gigabit-capable passive optical networks (XG-PON): Transmission convergence (TC) layer specification. [online]. 2010 [cit. 2014-03-29]. Dostupné z: http://www.itu.int/rec/T-REC-G.987.3

[12] HOOD, Dave a Elmar TROJER. *Gigabit-capable passive optical networks*. Hoboken: Wiley, 2011, ix, 431 p. ISBN 9781118155585.

[13] LAFATA, Pavel. *Pasivní optická přístupová síť EPON*. [online]. 2009 [cit. 2014-03-29]. Dostupné z: http://access.feld.cvut.cz/view.php?cisloclanku=2009050003

[14] LAFATA, Pavel a Matěj ROHLÍK. *Bezpečnostní rizika v současné generaci pasivních optických přístupových sítí*. [online]. 2010 [cit. 2014-03-29]. Dostupné z:http://www.elektrorevue.cz/cz/clanky/komunikacni-technologie/20/bezpecnostni-rizika-v-soucasne-generaci-pasivnich-optickych-pristupovych-siti/

[15] LAFATA, Pavel a Jiří VODRÁŽKA. *Pasivní optická síť 10GEPON*. [online]. 2010 [cit. 2014-03-29]. Dostupné z: http://www.elektrorevue.cz/cz/clanky/komunikacni-technologie/85/pasivni-opticka-sit-10gepon/

[16] ŠIFTA, Radim a Miloslav FILKA. *Simulace a měření vlnových multiplexů pro pasivní optické sítě*. [online]. 2011 [cit. 2014-03-29]. Dostupné z: http://elektrorevue.cz/cz/clanky/komunikacni-technologie/70/simulace-a-m--eni-vlnovych-multiplex--pro-pasivni-opticke-sit-/

[17] LAFATA, Pavel. *Pasivní optické sítě WDM-PON*. [online]. 2009 [cit. 2014-03-29]. Dostupné z: http://access.feld.cvut.cz/view.php?cisloclanku=2009050004

[18] HANÁČEK, Petr. *Bezpečnostní funkce v počítačových sítích*. [online]. 2011, č. 2 [cit. 2014-03-29]. Dostupné z: http://www.ics.muni.cz/bulletin/articles/171.html

[19] PIETILÄINEN, Antti a Olli-Pekka HIIRONEN. *Security Threats and Defense Models in EPON*. [online]. 2011 [cit. 2014-03-29]. Dostupné z: http://www.ieee802.org/3/efm/public/sep02/sec/Pietilainen_sec_1_0902.pdf

[20] IVÁNEK, Jiří. Základy kódování a kryptografie. [online]. 2006 [cit. 2014-03-29]. Dostupné z: http://www1.osu.cz/~klimesc/public/files/KODSI,%20ZKAKR/Zaklady%20kodovani%20a%20kryptografie.pdf

[21] GRYGÁREK, Petr. *Computer Networks Security*. [online]. 2009 [cit. 2014-03-29]. Dostupné z: http://wiki.cs.vsb.cz/pos/images/1/17/Security.pdf

[22] ZELINKA, Ivan. *Počítačové viry a bezpečnost počítačových systémů: Kryptologie*. [online]. [cit. 2014-03-29]. Dostupné z: http://arg.vsb.cz/Data/Vyuka/PVB12.pdf

[23] DUAN, Degong, Li LI a Honga LI. *Research on Downstream Encryption Scheme Based on Timestamp in GEPON Network*. Journal Of Networks [online]. 2012, roč. 7, č. 8 [cit. 2014-03-29]. Dostupné z: http://ojs.academypublisher.com/index.php/jnw/article/download/jnw070812661271/5274

[24] DOSTÁLEK, Libor, Marta VOHNOUTOVÁ a Miroslav KNOTEK. *Základy šifrování: symetrická a asymetrická kryptografie*. In: Flops [online]. 2011 [cit. 2014-03-29]. Dostupné z: http://www.flops.cz/zaklady-sifrovani-symetricka-a-asymetricka-kryptografie

[25] KOTON, Jaroslav, Petr ČÍKA a Vítězslav KŘIVÁNEK. *Samoopravné Reed-Solomonovy kódy*. [online]. 2006 [cit. 2014-03-29]. Dostupné z: http://access.feld.cvut.cz/view.php?cisloclanku=2006080002

[26] ROHLEDER, David a Václav LORENC. **802.1X - autentizace v počítačových sítích**. Zpravodaj ÚVT MU [online]. 2008, č. 1 [cit. 2014-03-30]. Dostupné z: http://www.ics.muni.cz/bulletin/articles/590.html

[27] MARCINIAK, Marian. Proceedings of 2003 5th International Conference on Transparent Optical Networks: collocated with 2nd Workshop on All-Optical Routing : June 30, in association with COST 266 and 2nd European Symposium on Photonic Crystals, June 30-July 1, in association with COST 288 and COST P11. 1. vyd. Piscataway, New Jersey: IEEE, c2003, s. 99-102. ISBN 07803781642. Dostupné z: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1264588

[28] GUPTA, Naveen, Divya DHAWAN a JAIN. *A Novel Physical Security in Wavelength Division Multiplexing Passive Optical Network (WDM-PON) Using Broadband Light Source.* International Journal of Scientific & Engineering Research [online]. 2013, roč. 4, č. 5 [cit. 2014-04-05]. Dostupné z: http://www.ijser.org/researchpaper/A-Novel-Physical-Security-in-Wavelength-Division-Multiplexing-Passive-Optical-Network.pdf

[29] THOMAS, Stephen a David WAGNER. *Insecurity in ATM-based passive optical networks*. [online]. 2002 [cit. 2014-04-05]. Dostupné z: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.16.2615&rep=rep1&type=pdf

[30] LG-Ericsson EA 1100. In: Profiber [online]. 2010 [cit. 2014-04-06]. Dostupné z: http://www.profiber.eu/LG-Ericsson-EA-1100/

[31] LG-Ericsson WPF 1132c. In: *Profiber* [online]. 2010 [cit. 2014-04-06]. Dostupné z: http://www.profiber.eu/LG-Ericsson-WPF-1132c/

[32] LG-Ericsson EARU 1112. In: *Profiber* [online]. 2010 [cit. 2014-04-06]. Dostupné z: http://www.profiber.eu/LG-Ericsson-EARU-1112/

[33] FTB-400. In: *Exfo* [online]. 2009 [cit. 2014-04-06]. Dostupné z: http://www.exfo.com/Documents/TechDocuments/Specification_Sheets/EXFO_spec-sheet_FTB-400_en.pdf

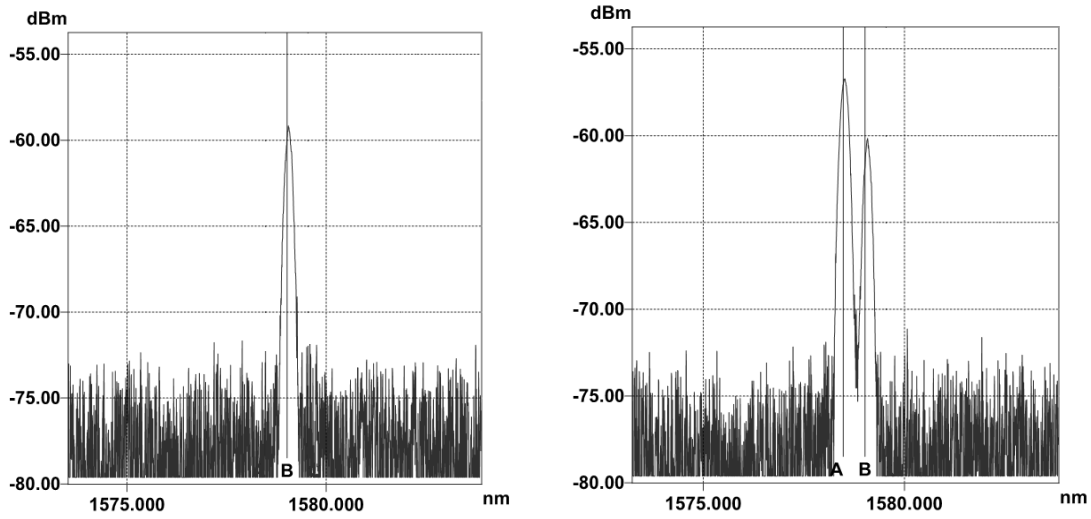
Seznam příloh

Příloha A: Grafy a naměřené hodnoty ze spektrálního analyzátoru, pro měření přeslechů při přímém zapojení analyzátoru do filtru AWG

Příloha B: Fotografie laboratorního pracoviště

Příloha C: Bloková schémata topologií použitých v prostředí Optiwave

Příloha A - Grafy a naměřené hodnoty ze spektrálního analyzátoru, pro měření přeslechů při přímém zapojení analyzátoru do filtru AWG



(a) Neaktivní jednotka na kanálu 6. **(b)** Aktivní jednotka na kanálu 6.

Obrázek A.1: Spektrum kanálu č. 7 před a po aktivaci jednotky na kanálu č. 6.

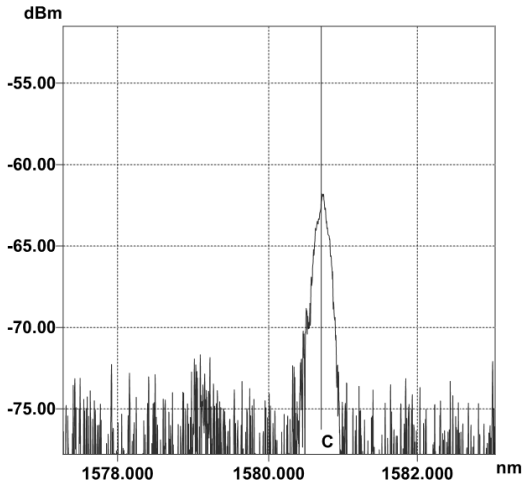
Špicka	Vlnová délka (nm)	Výkon (dBm)
A	-	-
B	1579,019	-59,90

(a) Neaktivní jednotka na kanálu 6.

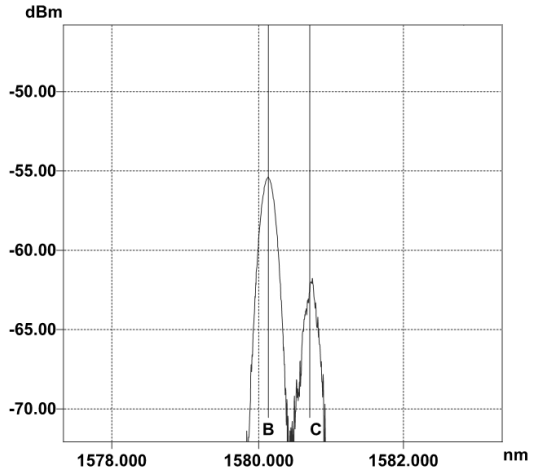
Špicka	Vlnová délka (nm)	Výkon (dBm)
A	1578,482	-57,07
B	1579,019	-61,88

(b) Aktivní jednotka na kanálu 6.

Tabulka A.1: Parametry spektra na kanálu č. 7 před a po aktivaci jednotky na kanálu č. 6.



(a) Neaktivní jednotka na kanálu 8.



(b) Aktivní jednotka na kanálu 8.

Obrázek A.2: Spektrum kanálu č. 9 před a po aktivaci jednotky na kanálu č. 8.

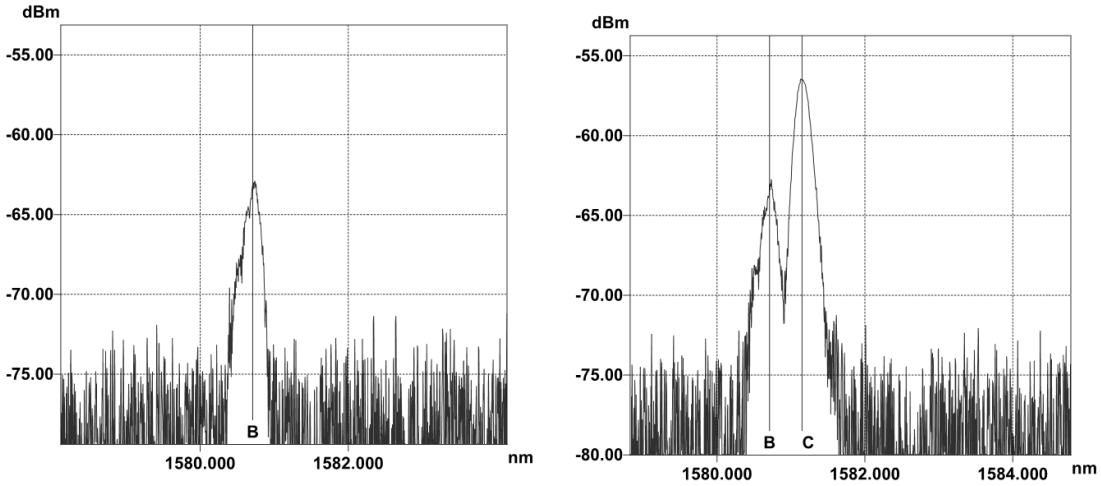
Špicka	Vlnová délka (nm)	Výkon (dBm)
B	-	-
C	1580,693	-62,42

(a) Neaktivní jednotka na kanálu 8.

Špicka	Vlnová délka (nm)	Výkon (dBm)
B	1580,129	-55,40
C	1580,693	-62,38

(b) Aktivní jednotka na kanálu 8.

Tabulka A.2: Parametry spektra na kanálu č.9 před a po aktivaci jednotky na kanálu č. 8.



(a) Neaktivní jednotka na kanálu 10. **(b)** Aktivní jednotka na kanálu 10.

Obrázek A.3: Spektrum kanálu č. 9 před a po aktivaci jednotky na kanálu č. 10.

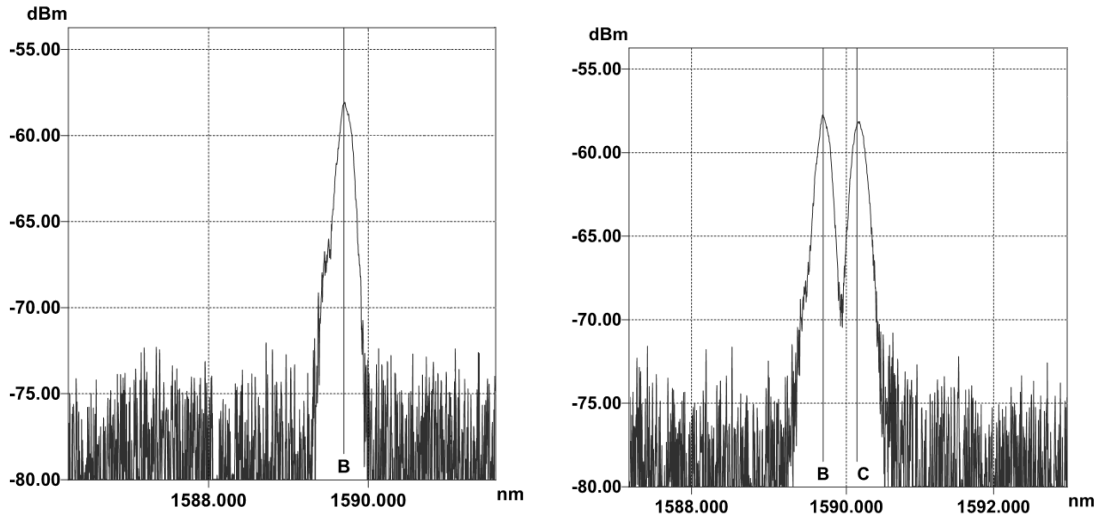
Špicka	Vlnová délka (nm)	Výkon (dBm)
B	1580,711	-62,30
C	-	-

(a) Neaktivní jednotka na kanálu 10.

Špicka	Vlnová délka (nm)	Výkon (dBm)
B	1580,711	-63,17
C	1581,151	-56,55

(b) Aktivní jednotka na kanálu 10.

Tabulka A.3: Parametry spektra na kanálu č. 9 před a po aktivaci jednotky na kanálu č. 10.



(a) Neaktivní jednotka na kanálu 21. **(b)** Aktivní jednotka na kanálu 21.

Obrázek A.4: Spektrum kanálu č. 20 před a po aktivaci jednotky na kanálu č. 21.

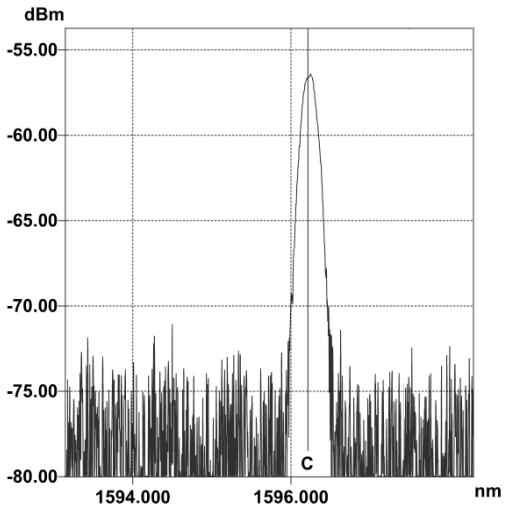
Špicka	Vlnová délka (nm)	Výkon (dBm)
B	1589,695	-58,13
C	-	-

(a) Neaktivní jednotka na kanálu 21.

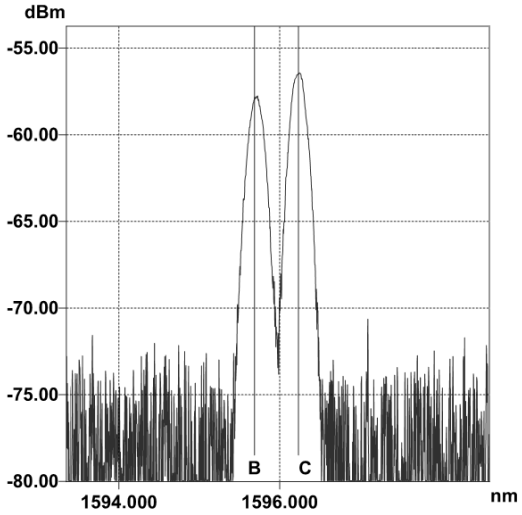
Špicka	Vlnová délka (nm)	Výkon (dBm)
B	1589,695	-57,86
C	1590,136	-58,32

(b) Aktivní jednotka na kanálu 21.

Tabulka A.4: Parametry spektra na kanálu č. 20 před a po aktivaci jednotky na kanálu č. 21.



(a) Neaktivní jednotka na kanálu 27.



(b) Aktivní jednotka na kanálu 27.

Obrázek A.5: Spektrum kanálu č. 28 před a po aktivaci jednotky na kanálu č. 27.

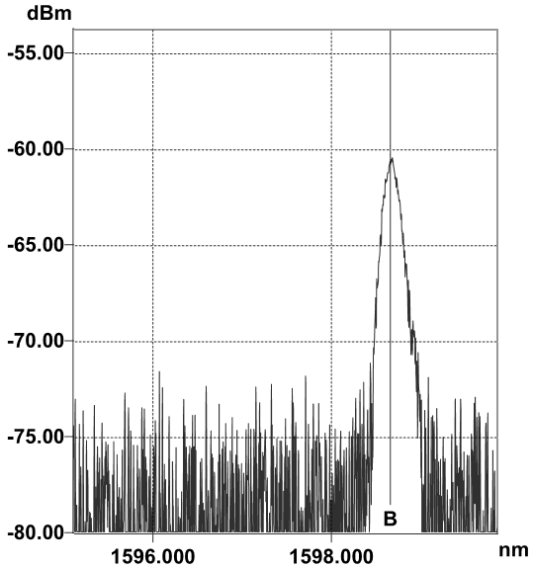
Špicka	Vlnová délka (nm)	Výkon (dBm)
B	-	-
C	1596,232	-56,64

(a) Neaktivní jednotka na kanálu 27.

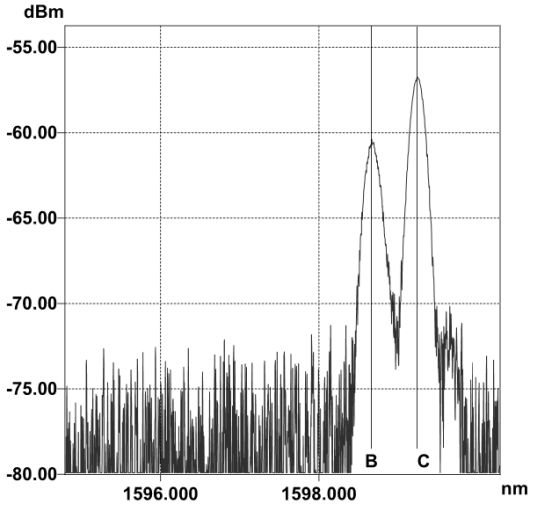
Špicka	Vlnová délka (nm)	Výkon (dBm)
B	1595,685	-57,93
C	1596,232	-56,50

(b) Aktivní jednotka na kanálu 27.

Tabulka A.5: Parametry spektra na kanálu č. 28 před a po aktivaci jednotky na kanálu č. 27.



(a) Neaktivní jednotka na kanálu 32.



(b) Aktivní jednotka na kanálu 32.

Obrázek A.6: Spektrum kanálu č. 31 před a po aktivaci jednotky na kanálu č. 32.

Špicka	Vlnová délka (nm)	Výkon (dBm)
B	1598,663	-60,74
C	-	-

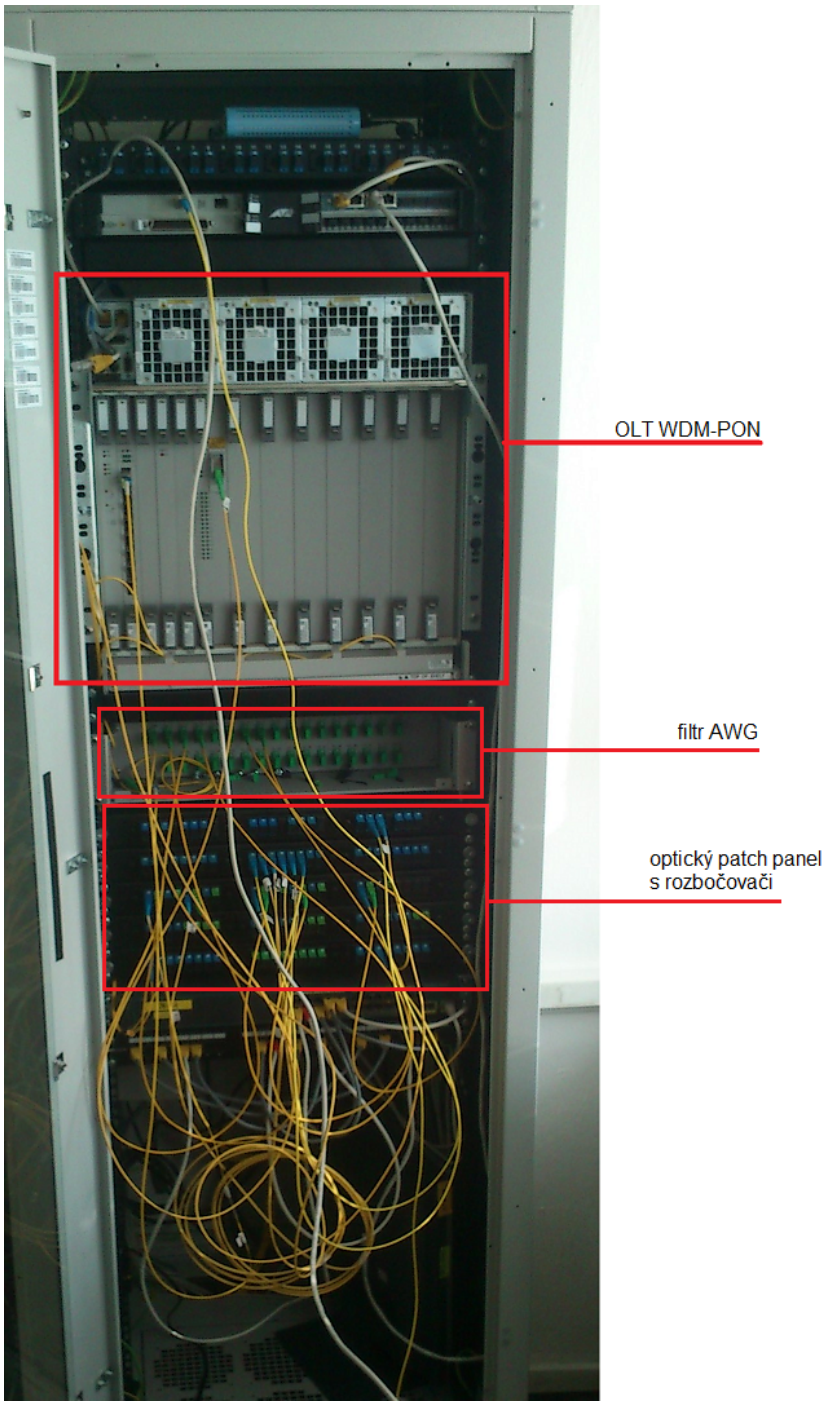
(a) Neaktivní jednotka na kanálu 32.

Špicka	Vlnová délka (nm)	Výkon (dBm)
B	1598,663	-60,56
C	1599,273	-56,79

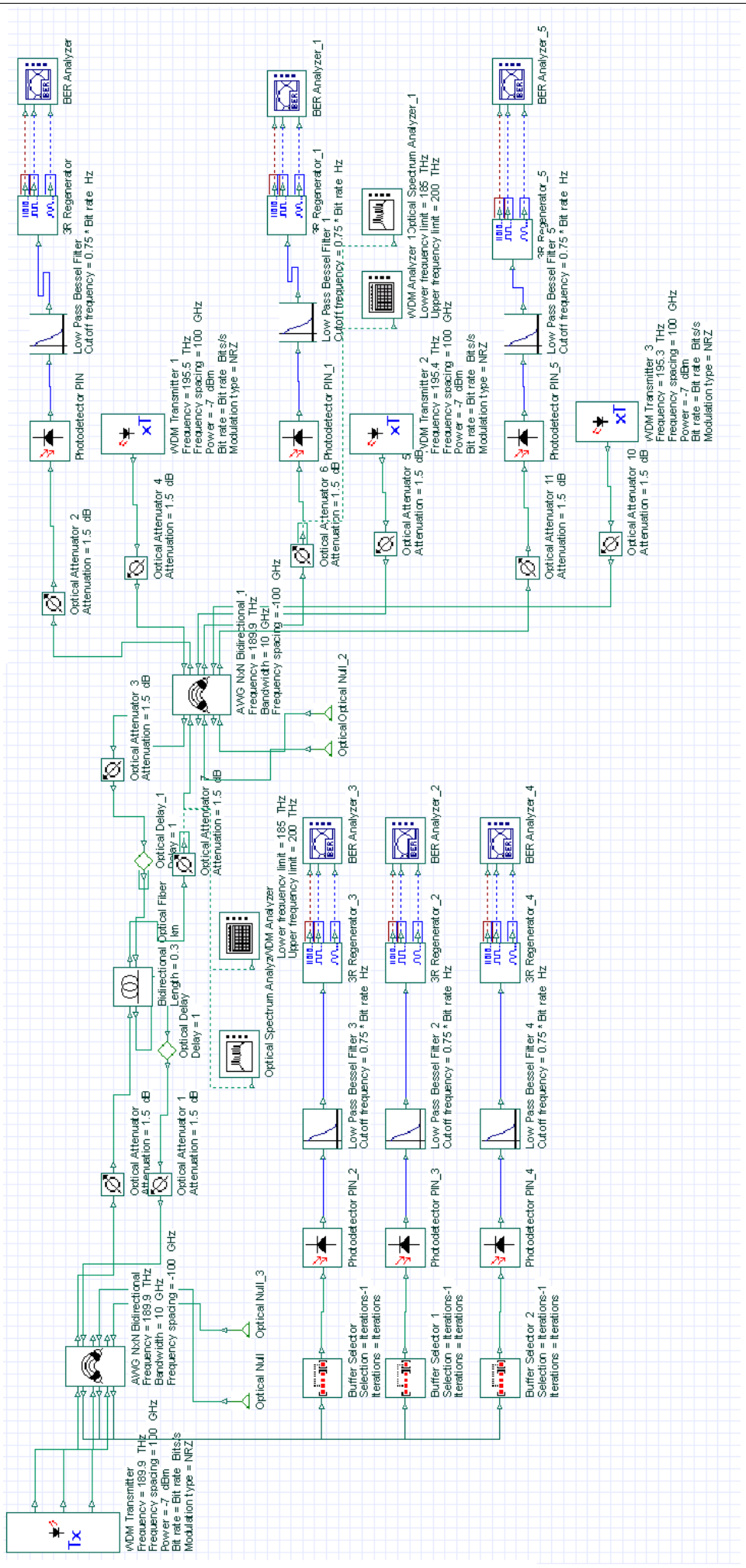
(b) Aktivní jednotka na kanálu 32.

Tabulka A.6: Parametry spektra na kanálu č. 31 před a po aktivaci jednotky na kanálu č. 32.

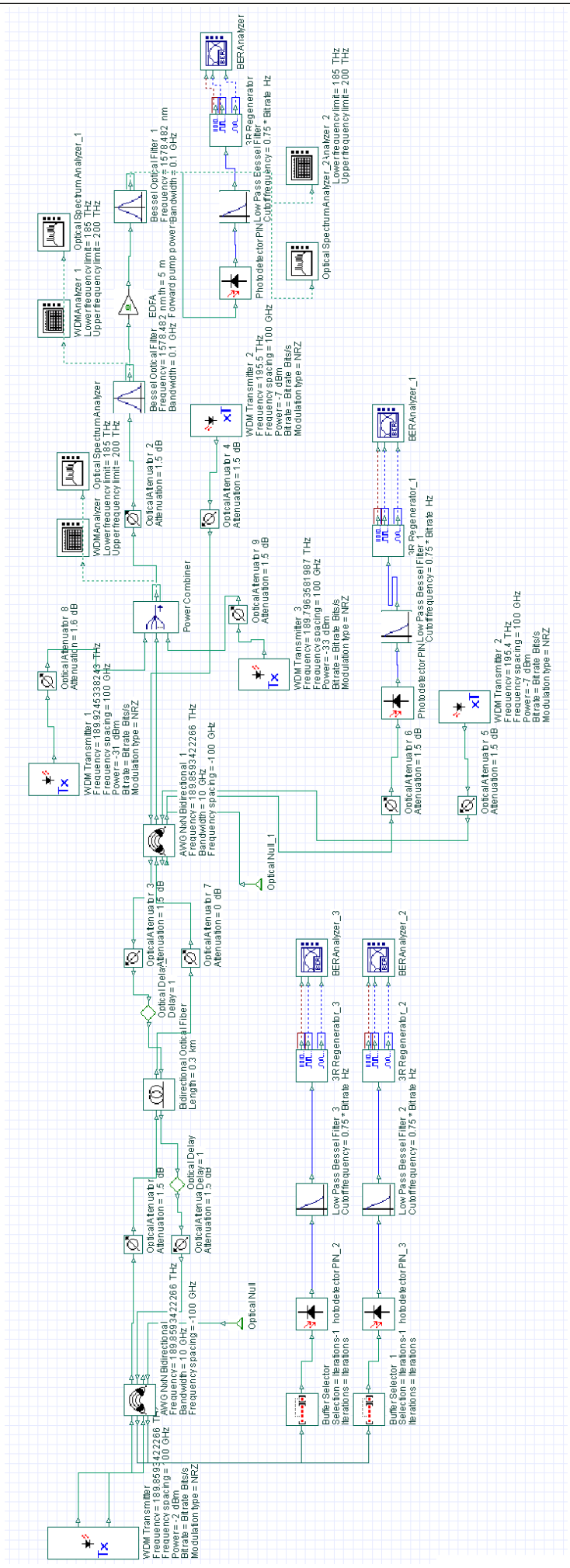
Příloha B - Fotografie pracoviště



Obrázek B.1: Hlavní rozvaděč N311.



Obrázek C.1: Schéma topologie č. 1 v Optiwave.



Obrázek C.2: Schéma topologie pro simulaci odposlechu s využitím přeslechu v Optiwave.